SBS Cyber Security

sbscybersecurity.co.uk

186 Cheetham Hill Road,
Manchester,
M8 8LW

M: 0161 827 1600

Mobile Device Usage Policy

Mobile devices will be issued to employees where **THE COMPANY** considers it necessary to enable the individual to perform the duties required of them during their employment. The decision as to whether any employee will be allocated a mobile device will be taken by a **PARTNER/COMPANY DIRECTOR.**

Our voice and data contract with Vodaphone/EE/O2/BT more than satisfies **THE COMPANY's** business requirements together with a generous provision for personal use. However, with irresponsible use it may be possible to exceed the contracted usage and excess charges will apply. This particularly applies to international roaming outside of Europe, where it is possible to incur costs of many thousands of pounds. Where these excessive costs are shown not to be business related, the user will be expected to reimburse **THE COMPANY.**

Mobile devices are relatively secure as they may be remotely managed by **THE COMPANY'S Mobile Server / RMM TOOLS.** All information forwarded to the mobile device is controlled in a secure way, but as security of client data is of the utmost importance to **THE COMPANY**, users are specifically asked to note the following:

1. Device Security

It is the responsibility of the user to keep the device safe and ensure use of the keypad lock and password facilities. The device must not be left where it may be accessed by non-authorised users.

For your information, the agreed default security settings are:

- Password length - minimum of 4 characters
- Number of retries - 4
- Keypad lockout time - 15 minutes

It is the responsibility of the user to keep the device free from damage.

Accidents obviously happen from time to time, but repeated carelessness will be monitored and a user may be asked to meet the cost of either a repair or replacement device in certain circumstances.

sbscybersecurity.co.uk
186 Cheetham Hill Road,
Manchester,
M8 8LW
M: 0161 827 1600

In the event of the loss of a device this should be reported immediately to **THIS PERSON on EXT / TELEPHONE NUMBER or THIS PERSON IN IT.** S/He will arrange for disconnection of the device and for a replacement to be issued.

To protect itself from loss of data the IT Department have the capability of remotely applying a 'factory reset' to all issued devices. **THE COMPANY** reserves the right to do this at its discretion.

It is essential that you inform the IT Department immediately if you lose control of your device (whether it be lost or stolen) - do not delay thinking that you may be able to recover the device.

2. Email Protocol

Users are reminded that they are subject to **THE COMPANY'S** policy governing emails (This can be found on **THE COMPANY'S Intranet/ in the Company Handbook**).

3. Leavers

When an employee leaves **THE COMPANY** their device must be surrendered together with the SIM. The mobile number will remain the property of **THE COMPANY**. It will not be permissible to transfer the mobile number to private ownership. Users are responsible for removing any private data from the device prior to handing it back to IT.

4. Personal Calls

THE COMPANY retains the right to monitor phone calls made via mobile devices and may ask individuals to pay for any calls that are not business related. In any case calls, should never be allowed to exceed one hour (see the second paragraph above).

5. Premium Rate Numbers

Calls made to premium rate numbers (including the speaking clock) will be blocked by the carrier.

6. Internet Access

Internet access via a mobile device is subject to the same protocols as would apply if you were on your PC. Usage will be monitored periodically going forward.

Mobile users are reminded that they are subject to the Group's policy governing internet access. (This can be found on **THE COMPANY'S Intranet/ in the Company Handbook**).

sbscybersecurity.co.uk
186 Cheetham Hill Road,
Manchester,
M8 8LW
M: 0161 827 1600

7. SMS (Short Message Service)/MMS (Multimedia Messaging Service)

It is accepted that there may be times when messages may need to be sent. However these should be kept to a minimum. As with personal calls, **THE COMPANY** retains the right to monitor mobile device usage and may ask individuals to pay for any messages that are not business related.

THE COMPANY does not permit texts to premium rate services as these are non-business related. Any service where a text is sent to a number usually 4/5 digits in length falls within this category. (This is a text message service charged at premium rate).

8. Data usage

Each of the Group's mobile devices are provided with a monthly data allowance. This agreed allowance forms part of **THE COMPANY'S** contract with the provider. The amount of UK data has been set higher than any foreseen business need. It is very unlikely that a user would exceed this allowance.

However, in some circumstances this allowance can be exceeded, for example, streaming video to the device or tethering to another device to provide internet connectivity to that device. This has the potential to attract charges of several thousand pounds per quarter. It is the users' responsibility to ensure this does not occur.

THE COMPANY reserves the right to charge users for excessive, non-business related, data usage.

You must not stream content unless you have confirmed a WI-Fi internet connection.

9. International Mobile Device Usage

Only make calls abroad that are work related and absolutely necessary.

International Data roaming charges remain extremely high in particular for Apple iPhones. Unless you have specific permission you must not enable data roaming whilst outside of the UK. Data functions on your device should be turned off for the duration of your trip – **THE IT DEPARTMENT** will assist you with this.

sbscybersecurity.co.uk
186 Cheetham Hill Road,
Manchester,
M8 8LW
M: 0161 827 1600

If you are going abroad and need to review your emails, IT will advise you on the best way forward.

NB If you need to access your voicemail when you are abroad you MUST ensure the facility is set up on your device whilst you are in the UK. This function cannot be accessed when you are abroad and cannot be performed remotely by **THE IT DEPARTMENT**. (Once you have set up voicemail in the UK the facility will work both in the UK and abroad).

To act as a reminder to you of the need to advise **THE IT DEPARTMENT and hey** will issue an email to all mobile device users on a monthly basis requesting details of any overseas travel plans.

These costs will be monitored going forward and any trends will be investigated.

10. Personal Application

Personal Apps should not be downloaded on to corporate devices as they inhibit **THE IT DEPARTMENT's** ability to support the device.

11. Personal Data

Personal data may be loaded on to your corporate device at your own risk. It may be necessary to reduce the amount of personal data storage to enable operating system upgrades and security patches. It is the user's responsibility to remove any personal data when requested.