Mobile Device Security

This is to remind staff about mobile device management and best practice. This is to reduce the risk of devices being lost, broken, stolen or hacked, it is also to outline the responsibility staff accept when being issued with a device.

Please read the below reminders to refresh yourself on best practice whether it is in the office, at home or any public location such as airport, trains, coffee shops, or in the car commuting.

Top mobile device reminders…..

Laptops and tablets should be carried and stored in the computer bag supplied by the Company to reduce the chance of accidental damage.

1. Mobile devices **should not be left unattended in the office or workplace overnight** (including weekends and holidays). Devices are the responsibility of their allocated owner and should either be in their possession or left in a locked drawer or cabinet in the office, out of sight.

2. **Do not leave your password notes in your laptop bag**, on your laptop, or near the device.

3. **Mobile devices should be stored in a hotel room safe** where available rather than left unattended in a hotel room, **or kept out of sight from windows** etc

4. **Devices should not be left unattended in a parked vehicle** unless there is no other option. They should be locked in the boot or out of sight while commuting. They should not be left in a vehicle overnight.

5. **Mobile devices are provided for business use by authorised employees**. Devices must not be loaned or be allowed to be used by others, this is to prevent any unauthorised software being installed and / or inappropriate web access.

6. Tracking or mobile device management software installed on the device must not be removed.

7. **Stolen devices must be reported to the police within 24 hours**, the incident report number is to then be given to the IT Department and HR.

8. Devices provided with protective casing should remain in the cases at all times (mobiles, tablets)

9. **Do not store usb or backup usb data within the same bag as the laptop**. As this creates the risk of you loosing both data sources at once. Always use an encrypted usb pen when transferring or saving confidential data onto it.

10. When at **any public location**, on plane / train, in a coffee shop, **use your privacy screen**, when this is not possible, **be vigilant** when logging in incase someone is looking over your shoulder.