Shropshire Community Health
NHS Trust

Policies, Procedures, Guidelines and Protocols

Document Details		
Title		Best Practice - Security Guidance for Mobile Devices (Phones and non-Windows Tablets)
Trust Ref No		1845-80442
Local Ref (optional)		N/A
Main points the document covers		Best Practice Security Guidance for Mobile Devices (Phones and non-Windows Tablets)
Who is the document aimed at?		All staff using Mobile Devices (Phones and non-Windows Tablets)
Owner		Andy Fletcher - IT Engineer
Approval process		
Who has been consulted in the development of this policy ?		Paul Stokes – IT Services Manager
Approved by (Committee/Director)		Jon Davis
Approval Date		18th February 2023
Initial Equality Impact Screening		Y
Full Equality Impact Assessment		No
Lead Director		Director of Finance
Category		
Sub Category		
Review date		18th February 2025
Distribution		
Who the policy will be distributed to		All staff using Mobile Devices (Phones and non-Windows Tablets)
Method		Electronic and Paper
Keywords		best practice security guidance for mobile devices, security guidance, mobile phone, tablet, mobile device, phones and tablets, 1845,
Document Links		
Required by CQC		
Other		
Amendments History		
No	Date	Amendment
1	09/09/2013	Original Doc V1.0
2	11/12/2015	Review and update V1.1
3	19/10/2017	Review and update V2.0
4	20/12/2018	Review and update V3.0
5	23/02/2021	Review and update V3.1
6	18/02/2023	Review and update v3.2

Best Practice - Security Guidance for Mobile Devices (Phones and non-Windows tablets)

- It is your responsibility to ensure that mobiles devices provided by the Trust are kept safe and secure at all times.

- You must be aware that mobile devices and any associated memory card(s) may not be encrypted and therefore not suitable for storing Personal Identifiable Data / Personal Confidential Data (PID / PCD) or any other sensitive information. This also applies to storage of audio recordings, photographs and videos captured by the mobile device.

- Any theft or loss of a mobile device should be immediately reported to your Line Manager and the IT Service Desk. If the mobile device has been stolen, report the theft to the police and to obtain an incident/crime reference number. You must also log the incident on the Trust's "Datix" system.

- All mobile devices must be configured with a security lock (PIN) code and encrypted; do not store the PIN or password on or with the mobile device or bag.

- You must not click on links in SMS (text messages), adverts on web pages or Emails on your mobile device from unknown senders or sources from which you are unsure, this is due to of the risk of opening malicious attachments or websites.

- Turn off Bluetooth when not using it to conserve battery power and also to prevent "Blue-jacking" – this is where a person nearby can take control of your mobile device.

- Where available, it is good practice to ensure that the operating system on your mobile device is updated to the latest version and patched with any security upgrades.

- You must not, under any circumstances, utilise remote back-up or storage facilities outside of the Trust infrastructure/environment e.g. **do not use** Dropbox, Google drive, box, etc. Apple devices must have iCloud services disabled.

- The installation of non-work related applications (Apps) on your Trust mobile device is not recommended. It is vital that all applications are installed via the official platform owner approved source (i.e. Apple Store, Play Store, Marketplace etc).

- You must not load pirated software, applications or any illegal content onto your Trust mobile device.

- Trust mobile devices should not be modified e.g. "rooted" or "jail-broken".

- You must not perform a factory reset on your mobile device as this can cause issues with the encryption on the device and will cause you to lose all of the data and settings.

- You must not, under any circumstances, store Personal Identifiable Data / Personal Confidential Data (PID / PCD) e.g. patient records, correspondence, appointment lists, on the mobile device or the memory card(s).

- Personal Identifiable Data / Personal Confidential Data (PID / PCD) must not be sent via SMS (Text messages).

- You must ensure that business (Trust) related information/data is sent through the corporate\NHSMail Email system and not via any personal Email account that may also be configured on the mobile device.

- Where a mobile device has been configured to access systems administered by the Trust such as NHSmail, Office 365, SharePoint regardless of whether the device is Trust or privately owned, the Trust's "IT Security Policy" will be enforced on that mobile device.

- Where appropriate (e.g. loss, theft or other security breach), the Trust reserves the right to perform a full remote 'wipe' on all mobile devices configured with access to the Trust's systems e.g. Email. This will be performed regardless of whether the mobile device is owned by Trust or privately owned by an individual.

- If the mobile device develops a fault which requires repair or replacement, you must notify the IT Department prior to returning it. The IT Department, where possible will attempt to reset the mobile device. Any memory card(s) must be removed from the mobile device before being returned to the supplier for repair or replacement.

- If your mobile device is to be replaced e.g. upgraded, the old mobile device must be returned to the IT Department so that the configuration for accessing the Trust's systems can be removed. This also applies to mobile devices that are privately owned but have been configured to access the Trust's systems.

- If you no longer need your Trust mobile device you must notify the IT Department and your Line Manager and then return it to IT for reconfiguration.

- If you wish to give your Trust mobile device to another member of the Trust, you must notify the IT Department and your Line Manager and return the phone to IT to be reconfigured before it is used by another member of staff.

- If you leave the Trust or change departments within the Trust, you or your Line Manager must notify the IT Department. You must hand your Trust mobile device to your Line Manager before leaving. The device will need to be returned to IT for reconfiguration before being reallocated.

- Any data stored solely on the Trust mobile device is done so at your own risk. It is your responsibility to ensure that anything important is backed up securely using trust approved storage (E.g. your U:\ drive or shared area on your work computer).

- Your Trust mobile device must not be used for internet access via USB, Wi-Fi or Bluetooth tethering unless agreed and configured by IT.

- Please ensure that you only use the genuine charger for your Trust mobile device. Non-genuine chargers can sometimes damage the device and increase the risk of fire. In addition, non-genuine chargers can cause security vulnerabilities.

- Do not connect your trust mobile device to public Wi-Fi hotspots or unsecured Wi-Fi networks. These are not always what they seem and can be used by criminals to intercept and steal your data, including personal information, emails, messages and passwords. This includes BT Openzone and BT Wi-Fi, which can easily be faked by fraudsters.

- When not using Wi-Fi on your trust mobile device, turn the Wi-Fi off. This is to prevent your trust mobile device from automatically and unintentionally connecting to Wi-Fi hotspots when the device is not in use. It will also save on your battery.

- Do not connect to, or install apps used for controlling IoT (Internet Of Things) devices, such as smart meters, smart locks, smart lighting or other smart appliances. These devices are known to have poor security on them and can provide a way of gaining unauthorized access to your trust mobile device.

- Please remove any apps which no longer function and are no longer available on the app store on your trust mobile device. Some of these apps may have been removed due to security flaws, malware issues or copyright infringements, but may still remain on your device even after they have been removed from the online app store.