South East Coast Ambulance Service NHS
NHS Foundation Trust

Mobile Device Policy

Contents

1 Statement of Aims and Objectives

1.1. South East Coast Ambulance Service NHS Foundation Trust is committed to the management and prevention of unacceptable risks to the Trust and other NHS Information assets through the use of Trust and non-Trust mobile computing facilities.

1.2. All staff that are permitted to use mobile computing equipment are subject to the requirements of the NHS Information Governance (IG) policy and procedures.

1.3. With the issue of Trust devices for mobile and remote working, there needs to be clear guidelines for staff for their safe and responsible use.

1.4. There are different categories of mobile devices covered by this policy, namely (but not exclusively), laptops, iPads, tablets and smartphones.

1.5. The key objectives of this policy are: -

- Ensure staff have a clear understanding of their responsibilities when using mobile devices.
- Explain the definitions of ‘personal use’ where they apply; and
- Outline the security processes when using the device.

2 Principles

2.1. Ownership

2.1.1. All corporately issued devices remain the property of the Trust, whether personally enabled or not, and staff will be expected to treat the device in accordance with the usage for which it was designed.

2.1.2. All devices will be encrypted and tablets/smartphones are to be protected by a minimum four-digit pin number. This pin number is to be treated like your network password or bank card pin and should not be divulged to anyone. The exception to this will be for staff who during their operational duties will need to dual use a tablet; for example, whilst treating a patient or driving. If you feel the pin number has been compromised, you should change it immediately and report its disclosure as a possible security incident.

2.1.3. You must not alter the configuration or customise the device by changing the hardware or operating system against the manufacturers or Trust’s initial configuration. This includes attempting to circumvent any security or Mobile Device Management (MDM) software installed on the device.

Attempts to do so will result in the device being automatically locked and the incident investigated as a security breach.

2.1.4. Where devices are defined as Corporately Owned Personally Enabled (COPE) devices, users are expected to ensure they are brought to work ready to be used – i.e., in working order, fully charged, and fitted to any specific case required for its purpose. This is particularly important for staff in operational roles where the opportunity to charge devices in vehicles or at remote locations may be limited, and specific cases are required for protection and/or infection control. The only exception to this is for Electronic Patient Clinical Record (EPCR) iPads as described in the EPCR Procedure as these devices may be secured in personal lockers on Trust premises.

2.1.5. All chargers supplied by the Trust are supplied in line with the required specifications. Users are expected to ensure any third-party accessory used meets the same criteria to avoid the risk of fire or damage to the device.

2.1.6. Wilful or malicious damage to devices is considered gross misconduct as outlined in the Trust's Disciplinary Procedure.

2.2. Personal Use Devices (COPE)

2.2.1. **iPads**: iPads are not connected directly to the main SECAmb computer network but are instead isolated by a Mobile Device Management (MDM) system. Therefore, whilst it is a corporately owned device and primarily for corporate use, an element of personal usage (as defined in 2.3.1) is permitted within the guidelines of this policy and will require a personal Apple ID.

2.2.2. **iPhones**: iPhones are protected by a Mobile Device Management (MDM) system, allowing the use of a personal Apple ID and the installation of personal Apps.

2.2.3. **Android Phones**: These are protected by a Mobile Device Management (MDM) system, allowing the use of a personal Google Account (in the format of firstname.surname@secamb.nhs.uk) and the installation of personal Apps.

2.3. Personal Use on Trust and non-Trust Devices

2.3.1. Although provided for business use, the Trust will permit some personal use provided it is reasonable and does not interfere with the main purpose and function of the device. Disciplinary action may be taken if the permitted use of the device is abused.

2.3.2. Personal usage does not include allowing non-SECAmb employees to use the device, including partners, spouses, family members and friends. This includes not using the device as a WIFI hotspot for personal use.

2.3.3. It does include being able to add your own Apple ID on Apple devices or Google Account ID on Android smartphones and the installation of personally bought applications and media for personal use.

2.3.4. Personal usage must not be contrary to the operation of the Trust, nor have the ability to bring the Trust into disrepute or be illegal in nature. The Trust has an obligation to report any illegal activity to the appropriate authorities.

2.3.5. Personal usage should be restricted to WIFI coverage where possible, to restrict the use of the Trust’s mobile data tariffs.

2.3.6. Excessive or inappropriate usage will be raised to the Multidisciplinary Panel in accordance with the Disciplinary Policy.

2.3.7. Laptops are not considered personally enabled devices. This is because they are directly connected to the SECAmb computer network. Only Trust provided laptops will be enabled for connectivity to the SECAmb computer network. All software must be owned and licenced by the Trust and have been reviewed via the Software Whitelisting procedure. There is no scope for personally owned software to be installed on Trust provided computers.

2.4. Security

2.4.1. Mobile devices, by their nature, will be taken outside of secure NHS environments, and can be subjected to additional security risks.

2.4.2. Because of this enhanced risk, password or pin protection alone is insufficient to guard against data loss, so each mobile device is encrypted. This means disassembly of the device and removal of any data storage components will not compromise the data held on it.

2.4.3. Users of mobile devices are expected to take all reasonable steps to keep them secure, as they would their own personal device. This includes (but not limited to) not leaving the device unattended on display (e.g., in a vehicle), ensuring the device is ‘locked’ when not using it, being aware of the surroundings when using the device to prevent theft. Do not keep the

PIN/password details with the device and do not reveal the PIN/password to anyone.

2.4.4. Any loss or theft must be handled in accordance with the Incident Reporting section below.

2.4.5. Potential threats to your mobile device security are detailed in Appendix A.

2.5. Threats to Your Mobile Device Security

2.5.1. If Applications are installed on a mobile device, then the member of staff responsible for the device needs to be mindful of Applications that can cause data leakage, are fake in origin, malicious or insecure. Only give Applications permissions they actually need to function. See Appendix A for further information.

3 Definitions

3.1. Mobile Devices

3.1.1. For the purpose of this policy, a mobile device is defined as a Trust-owned laptop, tablet computer or smartphone. The individual devices are defined below.

3.2. Laptop

3.2.1. A computer that is portable and suitable for use while travelling.

3.3. Tablet

3.3.1. A small portable computer that accepts input directly on to its screen rather than via a keyboard or mouse.

3.4. Smartphone

3.4.1. A mobile phone that performs many of the functions of a computer, typically having a touchscreen interface, internet access, and an operating system capable of running downloaded apps.

3.5. Corporately-Owned Personally-Enabled (COPE)

3.5.1. A principle that applies to some devices supplied, owned, and managed by the Trust where employees are allowed a reasonable amount of personal usage. This could include access to personal email and installation of their own Applications. COPE will only apply to devices that do not directly connect to the Trust's main network. These are usually identified by having a pin number or pattern to log on as opposed to a username and password.

3.5.2. **Bring Your Own Device (BYOD)** - Personal Devices. The Trust does not support BYOD.

3.5.3. **Personal Data -** Defined in the Trust Information Governance Policy.

3.5.4. **Sensitive Personal Data -** Defined in the Trust Information Governance Policy.

3.5.5. **Sensitive Information -** Defined in the Trust Information Governance Policy.

4 Responsibilities

4.1. **The Chief Executive Officer (CEO)** is ultimately accountable for the implementation of this Policy.

4.2. **The Trust Board** has responsibility to obtain assurance that the processes described work effectively and support the Board level public commitment to implementing the Mobile Device Policy.

4.3. **SIRO** has responsibility for implementing and managing information risks within the organisation. The SIRO role is mandatory for public sector organisations and organisations which are contracted to deliver services under the NHS Standard Contract.

4.4. **The Associate Director of IT** has delegated responsibility to ensure compliance with the Mobile Device Policy. The Associate Director of IT will report to the Trust Board and the Chief Executive Officer on matters relating to this Policy.

4.5. **The Senior Management Teams within the Trust** are responsible for ensuring compliance with this policy and the associated processes within their areas / stations / departments.

4.6. **All Staff** employed by the Trust are required to follow the principles outlined in this policy.

4.7. **Asset Register** All relevant mobile devices used for NHS business, or holding NHS information, must be uniquely identified and logged in the Trust's asset register.

4.8. **Accountability** Responsibility for the physical security of the Trust's registered mobile devices and their data will be assigned to individual staff members and tracked alongside the employment status of those individuals.

4.8.1. Staff assigned a Trust mobile device are required to ensure the device is maintained in respect of security or operating system updates to ensure protection of the Trust from cyber threats. See section Incident Reporting for the loss or theft of Trust mobile devices.

4.9. Management of Mobile Device Security Functionality

4.9.1. The installation and configuration of mobile device security functionality, including access control, encryption, and tamper resistance, will be undertaken by appropriately trained IT staff.

4.10. Security Accreditation

4.10.1. The Associate Director of IT will annually review the Trust's mobile device estate to ensure they continue to meet the requirements, and that the residual level of risk from their use is acceptable.

4.11. Physical

4.11.1. It is recommended that mobile devices, even when protected by encryption, should not be left in the care of any person who is not trusted to protect the information it contains.

4.12. Availability

4.12.1. IT will define the physical processes and procedures for the provision of mobile devices across the Trust, ensuring consistent standards. This will enable the continued availability of mobile devices in line with operational reasons, IT maintenance and security arrangements and pre-approved costs.

4.13. Remote Access

4.13.1. Remote access from a mobile device to NHS information systems must be authorised and achieved in accordance with the Trust's Remote Access Policy, NHS IG guidance, and any defined requirements for the protection or use of the NHS information service(s) concerned.

4.14. Data Storage and Use

4.14.1. All Trust mobile devices should be treated as holding sensitive data.

4.14.2. When a user receives or is required to download or store such data on a mobile device, as defined in section 3, this should be kept only to the minimum period for its effective business use.

4.14.3. The data must be removed immediately when there is no requirement for its use to minimise the risks should a breach occur.

4.15. Incident Reporting

4.15.1. Loss or theft of Trust mobile devices must be immediately reported to the IT Service Desk or the out of hours on call team for the device to either be tracked, wiped and/or barred by the service provider. An Incident Report (DIF1) must be completed in accordance with the Trust's Incident Reporting Procedure.

4.15.2. Theft will also need to be immediately reported to the Police and a crime reference number obtained.

4.15.3. Damage of Trust mobile devices must be reported to the IT Service Desk and an Incident Report (DIF1) completed in accordance with the Trust's Incident Reporting Procedure.

4.15.4. No mobile device can be taken abroad for recreational purposes and no device can be taken abroad without prior consent of the relevant Director.

4.15.5. Where this occurs, the IT department must be informed prior to travel and the incident reporting process must be followed in the event of any loss of information or hardware.

4.16. Secure Disposal and Reuse

4.17. Where possible users of Trust mobile devices will need to ensure data stored is securely erased before the device is reassigned for another purpose or disposed of when redundant.

4.18. Where a device is enabled for personal use, the Trust will not be liable for the cost of personal software or loss of any personal data. NHS IG guidance is available from NHS Connecting for Health for this purpose.

5 Education and training

5.1. Users need to be competent in the use of the devices they are issued. With the prevalence of tablets, smartphones, and laptops in daily life, the

Trust necessarily makes the assumption that staff are competent in the use of these devices unless otherwise informed.

5.2. Where staff identify they are not familiar or competent in the use of their device, escalation to line management will be required.

6 Monitoring compliance

6.1. The Information Governance Lead / Information Governance Manager (IG Lead / IG Manager) will monitor compliance with this policy as part of the annual system of information security audits. Where the Trust deems appropriate, internal audit will be asked to conduct information security audits.

7 Audit and Review (evaluating effectiveness)

7.1. The Information Governance Lead / Information Governance Manager will undertake required checks on, or an audit of, actual mobile device implementations based on approved security policies, as deemed necessary by the Associate Director of IT.

7.2. This policy will be reviewed annually under the authority of the Chief Executive. Associated information security standards will be subject to an on-going development and review programme as deemed appropriate from time to time by the Information Governance Lead / Information Governance Manager.

7.3. Notwithstanding the above specifics, all policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

7.4. Effectiveness will be reviewed using the tools set out in the Trust’s Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

7.5. This document will be reviewed in its entirety every year or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

7.6. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

8 References

- Data Protection Act 2018
- Computer Misuse Act 1990
- ISO/IEC 27002, Code of practice for information security management
- NHS Information Security Management Code of Practice
- NHS Digital Data Protection & Security Toolkit

9 Equality Analysis

9.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

9.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.

11. Quality Impact Assessment

11.1. A QIA has been completed and approved: QIR-270108

10 Appendix A - Threats to Your Mobile Device Security

10.1. Unsecure WIFI

10.1.1. Use a degree of caution when using free WIFI and never use it to access confidential or personal information. It is recommended that free WIFI is not used for personal services such as online banking or credit card services.

10.2. Spoofing

10.2.1. Spoofing describes a situation when a malicious party successfully impersonates another user or device. Hackers typically use spoofing to gain unauthorised access to a system or to sensitive information. There are several types of spoofing, including IP address spoofing, ARP spoofing, DNS server spoofing and email spoofing. It is recommended if there is a requirement to set up an account to use a free WIFI service that a 'new' password is used rather than one that has been used historically**.**

10.3. Phishing Attacks

10.3.1. Phishing is a form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels. The attacker uses phishing emails to distribute malicious links or attachments that can perform a variety of functions, including the extraction of login credentials or account information from victim's Trust email on your mobile device. Staff are advised to be vigilant, monitor email carefully and never click on unfamiliar email links**.**

10.4. Spyware

10.4.1. Spyware is a category of software which aims to steal personal or organisational information. It is done by performing a set of operations without appropriate user permissions, sometimes even covertly. General actions a spyware performs include advertising, collection of personal information and changing user configuration settings of the computer, so it is essential that staff do not allow others to install software on their mobile device**.**