



Mobile Device Policy

Version:	V2.0
Name of originator/ author:	Brian Croney
Responsible management group:	Heads of IM&T
Directorate/team accountable:	Finance and Corporate Services

Policy:	
Approved by:	Joint Partnership Policy Forum (JPPF)
Date approved:	12.11.18
Fit for purpose according to:	Heads of IM&T
Date approved:	

Date issued:	12.11.18
Date next review due:	11.11.21
Target audience:	All Staff
Replaces (version number):	V1.0

Equality Analysis Record	
Approved EA included	Dated: 01.11.18
Quality Impact Assessment	
Approved QIA included	Dated: 02.11.18

Document Control

Formal approval:

Final approval by:	Joint Partnership Policy Forum	
Version No. V2.00	Final	Date: 12.11.18
Responsible Management Group approval by:	Heads of IM&T	
Version No. V1.5	Final	Date:

Review/comments:

Person/ Committee	Comments	Version	Date

Circulation:

Records Management Database upload	12.11.18
Internal Stakeholders	
External Stakeholders	

Review Due by responsible Management Group:

Period	Every three years or sooner if new legislation, codes of practice or national standards are introduced	Date: 11.11.21
--------	--	----------------

Record Information:

Security Access/ Sensitivity	Official (Public Domain)
Where Held	Corporate Records Register
Disposal Method and Date	In line with national guidelines

Contents

Document Control	2
1 Statement of Aims and Objectives	4
2 Principles	4
3 Definitions	7
4 Responsibilities	9
5 Education and training.....	12
6 Monitoring compliance	12
7 Audit and Review (evaluating effectiveness)	12
8 Associated Trust Documentation	13
9 References	13
10 Equality Analysis	13
11 Quality Impact Assessment.....	15

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 devices for mobile 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. The device will be encrypted and protected by a minimum four digit pin number. This pin number is to be treated like your network password or bank card pin and not divulged to anyone. 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 try to materially alter the configuration or customise the device by changing the hardware or operating system against the manufacturer's or Trust's initial configuration. This includes attempting to circumvent any security or MDM software installed on the device. Attempts to do so could 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 or infection control. The application of this paragraph to ePCR iPads is modified by the Interim Electronic Patient Clinical record (ePCR) procedure paragraph 3.1 as these devices may be Secured in personal lockers on Trust premises

2.1.5. All chargers supplied by the Trust are supplied or approved by the device manufacturer. 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 would be considered gross misconduct as outlined in the Trust's Disciplinary Procedure

2.2. **Personal Use Devices (COPE)**

2.2.1. **iPads:** The iPad is not connected directly to the main network but is 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.

2.2.2. **iPhones:** Like the iPad, the iPhone is protected by MDM software allowing the use of a personal AppleID and the installation of personal Apps.

2.2.3. **Windows Phones:** These are also protected by MDM software and users can add their own Apps by using their own Microsoft Account ID.

2.3. **Personal Use**

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.

2.3.3. It does include being able to add your own Apple ID on Apple devices or Microsoft Account ID on Windows 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, not have the ability to bring the Trust into disrepute and be legal 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 Wi-Fi coverage where possible, in order to restrict the use of the Trust's data tariffs. Usage is monitored, excessive use will be queried, and staff could be asked to reimburse the Trust. Excessive use would be considered as being as at significant variance from Trust average use without reasonable justification.

2.3.6. Where it is identified a device has been used inappropriately or for personal gain, it is the responsibility of the line manager to review in conjunction with the nominated informatics representative. However, where it is identified that there is excessive use or there is evidence that the NHS may have been defrauded, the Counter Fraud team will be informed along with Human Resources and this could result in the individual being investigated under the Anti-Fraud and Bribery Policy and Disciplinary Policy which may lead to disciplinary action or prosecution.

2.3.7. Inappropriate use of any mobile device will be covered by the organisation's anti-fraud and bribery policy and disciplinary rules, this will include but is not limited to mobile devices being used to harass or bully other individuals, inappropriate photographs, moving images or photographs taken without permission, numerous and unsuitable text messages, used to call premium rate phone numbers, deliberate removal of security or encryption systems, used in disruptive or inappropriate manner breach of UK legislation etc.

2.4. **Non Personal use Devices**

2.4.1. **Laptops:** Laptops are not considered personally enabled devices. This is because they are directly connected to the corporate network and all software has to be owned and licenced by the Trust.

2.4.2. **Microsoft Tablets:** Microsoft tablets (such as the Surface Pro) are directly connected and act as a laptop alternative device. Therefore the same rules as laptops apply and there is no personal use element.

2.5. **Security**

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

2.5.2. 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.

2.5.3. Additionally, COPE devices, protected by the MDM system, will have their content automatically wiped after 10 incorrect PIN attempts.

2.5.4. 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.

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

2.6. Threats to Your Mobile Device Security

- 2.6.1. 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.

2.7. Unsecure WIFI

- 2.7.1. 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.

2.8. Spoofing

- 2.8.1. 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 that staff 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.

2.9. Phishing Attacks

- 2.9.1. 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 victims. Trust email on your mobile device is readily available. Staff are advised to be vigilant, monitor email carefully and never click on unfamiliar email links.

2.10. Spyware

- 2.11. 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

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 laptop computer, sometimes referred to as a notebook computer, is a battery or AC-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in a non-office environment such as on aeroplanes, in libraries, temporary offices, and at meetings.

- 3.3. **Tablet Computer**

- 3.3.1. A portable computer that uses a touchscreen as its primary input. Most tablets are slightly smaller, weigh less and are often less powerful than the average laptop. While some tablets include fold out keyboards others only offer touchscreen input. Some tablet devices can connect directly to the Trust network whilst others cannot and are managed by separate Mobile Device Management (MDM) software.

- 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 applications (Apps).

- 3.5. **COPE**

- 3.5.1. Corporate-Owned Personally-Enabled (COPE), a principle that applies to some devices supplied, owned and managed by the Trust that employees are also allow 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 to log on as opposed to a user name and password.

- 3.5.2. **Personal Devices (non-Trust owned)**

- 3.5.3. The Trust Executive Team took the decision in December 2017 to allow access to all Office 365 services from any non-Trust or Trust owned device from any location which needs to be connected to the internet. This include smartphones, tablets, desktops, laptops, terminals and home automation devices and services. Reference can be made to "Guidance for access to Office 365 on non-Trust devices Policy" dated October 2018 for further information.

- 3.6. **Personal Data**

- 3.6.1. Any information that alone or in combination with other information, may lead to the identity of a living individual.

3.7. **Sensitive Personal Data**

3.7.1. Defined in the Data Protection Act 2018 as:

- the racial or ethnic origin of the data subject,
- political opinions, religious beliefs or other beliefs of a similar nature,
- whether a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),
- physical or mental health condition,
- sexual life,
- the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

3.8. **Sensitive Information**

3.9. Information that might be exempt from disclosure under the Freedom of Information Act 2000 (e.g. commercially sensitive; for future publication; affecting national security etc.); or that may bring the Trust into disrepute

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. **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.

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

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

4.6. **Baseline Information Security Standards**

4.6.1. NHS Chief Executives are responsible for the Information Governance (IG) of activities undertaken by their organisations and includes the confidentiality, integrity and availability of NHS information including patient data.

- 4.6.2. The policy is equally applicable to NHS contractors, services providers and other organisations or agencies that use mobile devices to process NHS information in the performance of their duties. The following IG principles and policy should be demonstrated when using mobile devices:

- 4.7. **Registration**

- 4.7.1. All mobile devices used for NHS business, or holding NHS information, must be uniquely identified and logged in the Trust's asset register as IG security-relevant items.

- 4.8. **Accountability**

- 4.8.1. Responsibility for the 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.

- 4.9. **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. **Authorisation**

- 4.11.1. Regardless of a mobile device's ownership, the use of any equipment outside the Trust's business premises for the processing of NHS information must be authorised by the relevant Director or Head of Department. Where the processing of NHS patient information is proposed on mobile devices, additional authorisation must be obtained from the Trust's Caldicott Guardian.

- 4.12. **Physical**

- 4.12.1. 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.

- 4.13. **Availability**

- 4.13.1. Continued availability of mobile devices, for operational reasons and because of the costs of replacement, will mean that consistent standards of physical and procedural protection will be required for all devices used by the Trust. These will be defined by the IT department and relevant staff and contractors made aware.

4.14. Remote Access

- 4.14.1. Remote access from a mobile device to NHS information systems must be 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.

4.15. Data Storage and Use

- 4.15.1. Sensitive data, including that relating to patients, will not ordinarily be stored on a Trust mobile device. Such data will normally be saved to the Trust's secured network drive, where security access and access level authorisation exists. When it becomes necessary to store such data, as defined in section 3, on a mobile device, this should be kept to the minimum amount required for its effective business use. The data must be removed immediately when there is no requirement for its use in order to minimise the risks should a breach occur. In addition, the device must be equipped with appropriate encryption software when it is to be used to store such data.

4.16. Incident Reporting

- 4.16.1. Loss or theft of Trust mobile devices must be reported to the IT Service Desk in order for the device to either be tracked, wiped and/or barred by the service provider. Theft will also need to immediately reported to the Police and a reference obtained. In either case an Incident Report (IRW-1) completed in accordance with the Trust's Incident Reporting Procedure.
- 4.16.2. Damage of Trust mobile devices must be reported to the IT Service Desk and an Incident Report (IRW-1) completed in accordance with the Trust's Incident Reporting Procedure.
- 4.16.3. Trust mobile devices not enabled for personal use must not be used for recreational purposes. No device must be taken on holiday without prior consent of the relevant Director. Where this occurs the IT department must be informed prior to travel and the same incident reporting process must be followed in the event of any loss of information or hardware.
- 4.16.4. The process for reporting the loss, theft or damage of Trust mobile devices can be found in the Airwatch Secure Content Locker (Corporate Content) on any enrolled mobile device.

4.17. Secure Disposal and Reuse

- 4.18. Data stored on Trust mobile devices must be securely erased before the device is reassigned for another purpose or disposed of when redundant. Failure to erase data securely may result in that data being available to the new owner/ user of the device.

- 4.19. Where a device is enabled for personal use, the Trust will not be liable for the loss of any personal data or software. 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 makes the assumption that staff are generally competent in the use of these devices unless otherwise informed.
- 5.2. Where staff indicates they are not familiar or competent in the use of their device, training will be provided.
- 5.3. Training will also be provided in the use of the specific software applications that staff are required to use in their daily routine. This training will be appropriate to level of complexity so could range from a formal course, one-to-one instruction, demonstration by a 'super user' to the provision of a written guide.

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 Associated Trust Documentation

- 8.1. Information Governance Policy
- 8.2. Information Security and Risk Management Policy
- 8.3. Removable Media Information Security Policy
- 8.4. Flexible Working Policy
- 8.5. Internet and Email Policy
- 8.6. Social Media Policy
- 8.7. Guidance for access to Office 365 on non-Trust devices
- 8.8. Disciplinary Policy and Procedure
- 8.9. Patient Photographic and Video Recording Policy
- 8.10. Data Protection Policy

9 References

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

10 Equality Analysis

- 10.1. 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.

- 10.2. 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.

Name of author and role	Brian Croney IT Service Manager		
Directorate	Finance	Date of analysis:	11/10/18
Name of policy being analysed	Mobile Device Policy		
Names of those involved in this EA			

1. Trust policies and procedures should support the requirements of the Equality Duty within the Equality Act:	<ul style="list-style-type: none"> • Eliminate discrimination, harassment and victimisation; • Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it; • Foster good relations between persons who share a relevant protected characteristic and persons who do not share it. 	In submitting this form, you are confirming that you have taken all reasonable steps to ensure that the requirements of the Equality Duty are properly considered.
---	---	--

2. When considering whether the processes outlined in your document may adversely impact on anyone, is there any existing research or information that you have taken into account?	<p>For example:</p> <ul style="list-style-type: none"> • Local or national research • National health data • Local demographics • SECamb race equality data • Work undertaken for previous EAs 	<p>If so, please give details:</p> <p>The Trust's Equality, Diversity and Inclusion Policy was reviewed during the production of this policy and reference made to the previous EA dated 24/04/15</p>
--	---	---


3. Do the processes described have an impact on anyone's human rights?	No
---	----

4. What are the outcomes of the EA in relation to people with protected characteristics?			
Protected characteristic	Impact Positive/Neutral/Negative	Protected characteristic	Impact Positive/Neutral/Negative
Age	Neutral	Race	Neutral

Disability	Neutral	Religion or belief	Neutral
Gender reassignment	Neutral	Sex	Neutral
Marriage and civil partnership	Neutral	Sexual orientation	Neutral
Pregnancy and maternity	Neutral		

5. Mitigating negative impacts:

If any negative impacts have been identified, an Equality Analysis Action Plan must be completed and attached to the EA Record. A template for the action plan is available in the [Equality Analysis Guidance](#) on the Trust's website. Please contact inclusion@secamb.nhs.uk for support and guidance.

EA Sign off	
EA checkpoint (Inclusion Working Group member, preferably from your Directorate)	Isobel Allen
By signing this, I confirm that I am satisfied the EA process detailed on this form and the work it refers to are non-discriminatory and support the aims of the Equality Act 2010 as outlined in section 1 above.	
Signed: 	Date: 01.11.18

11 Quality Impact Assessment

- 12.1. A QIA has been completed and approved by the Nursing and Quality Directorate. It is available from them or from the Corporate Governance Team.
- 12.2. No negative impacts on patient safety were identified.