Mobile Working Policy

Version: 1.0

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	This document describes the Information Security requirements for "Mobile Working" on Solent Health NHS Trust (the Trust) mobile computing devices and remote access facilities.
Document Type	[x] Policy [ ] SOP [ ] Guideline
Reference Number	Solent NHST/Policy/ IT01
Version	1.0
Name of Approving Committees/Groups	Working Differently Programme Board, Policy Steering Group and Trust Management Team Meeting
Operational Date	January 2020
Document Review Date	January 2023
Document Sponsor (Name & Job Title)	Chief Operating Officer, Southampton and County wide
Document Manager (Name & Job Title)	• Director of IT • Head of ICT Service Delivery • Head of Information Governance
Document developed in consultation with	Working Differently Board , ICT Team, IG Team
Intranet Location	Business Zone > Policies, SOPs and Clinical Guidelines
Website Location	Publication Scheme
Keywords (for website/intranet uploading)	Data, information, media, mobile working, anti-virus, malicious software ICT security, disposal of media and equipment, virus, computer, storage, connections, email, internet, portable devices, workstation, laptop, tablet, USB, encryption, McAfee, information assurance, confidentiality, integrity, availability, incidents, smart phone, network connection, Blackberry, Passwords, PINs, removable media, memory devices, PID, Sensitive Electronic data (SED), WEP, Wireless Protected Access (WPA), WPA2, Wi-Fi, IT01, Policy

Version Control

Change Record

Date	Author	Version	Page	Reason for Change
05/02/2015	Mike Franks	0.1		Original Draft
10/02/2015	Lisa Hodgson	0.2		Review comments
11/04/2016	Rebecca Lester	0.3		Review of original and edit to reflect updated requirements
13/04/2016	Rebecca Lester	0.4	9	Remote working addition
28/04/2016	Peter Grimley	0.5	9,11	Remote working wording change, Port Replicators addition
05/05/2016	Peter Grimley	0.6	1,14	Vision added, Day in the life appendix added
15/09/2016	Julie Hardy	0.7	2, 15	Summary of Policy, Equality Impact Assessment added
29/09/16	Julie Hardy	0.8	2, 7,11,12	Clarity that mobile devices can be left on desks overnight in secure Solent office/location
30/09/16	Julie Hardy	1.0		Amendments following Policy Steering Group. Formatted improved and roles added/updated. Appendix revised and CGI policy included.
30/12/2019	Dawn Day	1..0	3,5,6,7,8, 9,10,11	Updated policy document template and text amended to reflect mobile device includes mobile phones and laptops.

Reviewers/contributors

Name	Position	Version Reviewed & Date
Working Differently Programme Board	Approved	11/04/16
Policy Steering Group	Approved subject to amendments	29/09/16

EXECUTIVE SUMMARY OF POLICY

The key objective of this policy is to provide an appropriate governance framework for mobile working and in particular:

- enabling the workforce to be mobile and flexible
- ensure risks are effectively managed to protect the Trust, staff, patients, data and emerging threats.
- compliance to the ICT Security Policy.
- protecting electronic data

The document outlines the roles and responsibility of individual staff working within the Trust regarding the management of hardware and information governance. This document provides guidance to help staff maximise the potential of remote and flexible working which in turn enables more time to care. Mobile working reduces the travel costs to the Trust and also enables staff at any site, or working from any location, to update notes whilst working within secure environment.

The key messages are that staff must always be aware of threats to system security through hardware cyber breaches or errors when working with Personal Identifiable Data (PID). Staff must always be aware of what can be viewed on their device, and at all times protect data from others.

Devices must be connected to the network at least once a month to ensure that the devices are installed with the most up to date data security patches.

Mobile Devices are the responsibility of the individual user, and this covers mobile phones as well as laptops. It is the responsibility of the staff member to keep the devices safe and not vulnerable to theft or access by people.

This policy applies to all Trust employees, volunteers and contractors.

This policy covers users that work on Trust owned devices, Virtual Private Networks (VPN) or mobile devices configured for work purposes. From this policy, services need to create a Standard Operating Procedure which conforms to this legislation.

Table of Contents

Mobile Working Policy

1. Vision

1.1 The Trust's vision to develop its mobile working capability is reflected in the corporate objectives:

- To place people who use the Trust's services at the centre of decision making with key priorities being :
  - To deliver service and financial performance and cost improvement programmes safely and confidently, with key priorities including increasing IT capability through the purchase of systems to enhance interoperability.
  - Expanding mobile working to increase service productivity and support estates rationalisation

1.2 Through investment in IT and Clinical systems, it is now possible to provide staff with a stable IT platform and the ability to work in a more dynamic and mobile way.

1.3 For a number of years, staff have reportedly felt frustrated at having to travel, often long distances to return to a base to complete records, collect emails and undertake other similar tasks. The introduction of mobile technology will enable staff to be able to plan their diary and working day without the need to return to base thus reducing unnecessary travel.

1.4 Consider where appropriate moving to a culture in which undertaking meetings face to face becomes the exception rather than the norm. All staff are asked to always consider using the Skype for Business (Lync) in the first instance. Exceptions should include staff with special requirements such as hearing impaired staff or where English is not first language etc.

1.5 It has always been acknowledged that a single corporate policy would not be appropriate for every service. Therefore the information within this policy should provide the overarching security and management information. Each service will be required to develop a Standard Operational Procedure which defines how the service will work in a more dynamic way and manage clinical supervision and team development.

2. Introduction

2.1. The Trust continues to take advantage of the benefits offered by technology, enabling the workforce to be mobile and flexible.

2.2. With the advantage of using mobile devices there are associated known risks which must be effectively managed to protect the Trust, staff, patients, data and emerging threats.

2.3. Any user of a mobile device will comply with this policy in addition to the ICT Security Policy.

2.4. This policy provides instruction that must be followed whilst using, transporting and acting as custodian of Trust devices. It describes how data must be protected electronically.

3. Scope

This policy applies to locum, permanent, and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers), bank staff, Non-Executive Directors and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, agency workers, and other workers who are assigned to Solent NHS Trust.

4. Definitions

4.1. **Computer Virus** is a malware program that, when executed, replicates by inserting copies of it into other computer programs, when this replication succeeds the affected areas are then said to be 'infected'.

4.2. **Mobile Computing** is known as human/computer interaction by which a computer (notebook/iPAD/smart phone) is expected to be transported during normal usage.

4.3. **Anti-Virus Software** is computer software used to prevent, detect and remove malicious software.

4.4. **Sensitive Electronic Data (SED)** is information that can be used on its own or with other information to identify individual or business data.

5. Duties/Responsibilities

5.1. **Responsibility** for ICT Security rests with the **Chief Executive.**

5.2. **Chief Executive** has delegated responsibility to the **Senior Information Risk Officer**.

5.3. The **ICT Security Specialist (within our IT Provider)** is responsible for developing, managing and implementing ICT Security policies/processes on a daily basis.

5.4. The **ICT Department (NHS & our IT Provider)** will:

5.4.1. ensure that Trust issued devices are encrypted unless an exceptional case for not doing so has been approved

5.4.2. provide advice on implementation of this policy as requested

5.4.3. ensure that User access rights are correctly implemented

5.5. **Line Managers** are responsible for ensuring that:

5.5.1. staff comply with this policy and associated procedures and take action as appropriate against any member of staff in breach of this policy

5.5.2. notify any suspected breaches of this policy to Information Governance via the electronic reporting system

5.5.3. all Trust devices are returned by owners leaving the Trust to the ICT Department

5.6. **Trust Staff** must without exception:

- abide by this and associated policies & procedures, understand that failure to comply with the rules and regulations contained in this policy may result in disciplinary action
- report any suspected breaches of this policy to their line manager or the ICT Department
- report the loss/theft of a device to their line manager, ICT Department via the ICT Helpdesk and the log an incident on the Trust Incident Reporting System at the earliest possible opportunity

6. Process

6.1. Physical Security

Trust Staff shall accept full responsibility for the security of the device (laptop, IPad, surface Go etc and mobile phone), taking necessary precautions to avoid loss, theft or damage. Staff must:

- take all reasonable care to prevent the theft or loss of their device. The device must not be left unattended in a public place or left in/ on view in a vehicle. When transporting it, ensure that it is safely stowed out of sight. Devices must also not be left in a car overnight.
- be extra vigilant if using any device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of Trust stored information by a third party "overlooking"
- do not leave the device unattended for any reason whilst working on it unless session is "locked" and it is in a safe working place. To lock the device use the Ctrl Alt Del keys and select "Lock Computer" or Windows Key and L button also lock the screen
- ensure that other un-authorised users are not given access to the device or the data it contains

6.2. Passwords & PIN Codes

Passwords are an integral part of Access Control which is enforced by the Operating System (e.g. Windows). Enforcement means that passwords shall be a combination of letters and

digits of a pre-determined length and combination of characters, typically using the upper and lower case of the keyboard.

- Passwords and/or PINs should not normally be written down. Regular password changes reduce the risk of unauthorised access to the machine and therefore passwords must be changed at least every 90 days, but more frequently if required.

6.3. **Approved Use**

Trust devices will be supplied with pre-installed software that has been procured by the ICT Department and approved by the Trust. Users must not attempt to install any software including their own privately procured and licensed software onto any Trust device. Under no circumstances is Trust licensed software to be upgraded, deleted or copied by users. Users are not permitted to attach additional unauthorised hardware or in any way change the original hardware configuration of the device, without prior approval from the ICT Department.

6.4. **Anti-Virus Software**

Trust devices capable of running Anti-Virus software will be supplied with it pre-installed. It is the user's responsibility to ensure it is updated regularly, achieved by connecting the device to the Trust network on a regular basis. The pre-installed version of Anti-Virus Software is the only approved product that may be used to protect the device. Machines regularly connecting to the Trust networks will automatically scan and update on connecting.

6.5. **Storage of Data**

Data should not normally be saved or stored onto the local drives i.e. the C:\ drive. This drive is only accessible to the device user and is not backed up and therefore is not secure. Data should normally be saved or transferred to network drives (of any device including desktops) i.e. shared file storage areas or the user/owners H:drive. Where data is stored locally owners/users should regularly upload the data to network drives and delete data held locally.

6.6. **Protection of Sensitive Electronic Data (SED)/Encryption**

Where departments or individuals process SED on mobile devices they must do so in accordance with the specific encryption requirements of the relevant part of the Information Security Policy and Encryption Policy.

- All trust issued laptops are to be encrypted.

- Any mobile device issued by the Trust, or personal devices shall be managed by the approved Mobile Device Management (MDM) solution, which allows email, contacts and calendars to be synchronised to the device. If the device is lost or stolen a remote wipe can be sent to clear data off the device.

6.7. **USB Memory Devices**

The Trust has mandated that the only approved method to transfer personally identifiable data is using an encrypted USB data stick. The Information Security Policy and Encryption Policy supports USB memory devices.

6.8. **Remote Access**

All devices will be delivered to staff fully configured to enable the user to connect back to the Trust network via Wireless/3G/4G using Virtual Private Network (VPN).

Connecting through the VPN creates a secure tunnel back to the Trust network and the user will have the same access and functionality as they would when in the office.

6.9. **Monitoring Usage/Audit**

The Trust will monitor the contents of files stored on Trust Devices, irrespective of whether they are for Trust or personal use, in order to detect any misuse and identify users not complying with this policy. This ensures the protection of Trust patients/staff, its reputation, and compliance with the General Data Protection Regulation (GDPR).

6.10. **Audit and Monitoring Controls**

Trust systems will log events that have a relevance to potential breaches of security. The minimum retention period for all logs is normally one year unless a different period has been agreed with the ICT Department and our IT Provider. This is documented in the Solent NHS Trust Security Management Plan (Appendix 5).

6.11. Events that should be logged:

- log-on attempts - user IDs, dates and times, successes/failures
- creation, amendment and deletion of data - recording User IDs, dates and times
- access and use of IT resources including, but not limited to, internet and Email usage and printer activities

6.12. **Investigations/Disciplinary Proceedings**

The ICT Department and our IT provider are authorised to independently investigate all suspicious, inappropriate or illegal activity involving Trust IT equipment and data however it may come to their attention.

No other members of staff are authorised to conduct such activities involving IT equipment or data unless directed by the SIRO.

6.13. **Return of Devices**

Staff leaving the Trust must return the device (including bags, cables, USB sticks and headsets) to their line manager. A leaver, in relation to device management, is classed as anyone who is not going to be actively working for the Trust for more than 5 weeks. This could be someone going on maternity leave, long term sick leave, a secondment or actually leaving the Trust.

If laptops, mobiles or power cables are not returned, there will be an additional change to the service line/user. £1200 per laptop, £90 per cable and £200 per mobile phone. Line managers are responsible for ensuring that the device is returned to the ICT Department.

6.14. **Wireless & Cordless Computing Connections**

All devices are equipped with wireless connection interfaces and can be connected to enable access via VPN to Trust systems.

7. Remote Working

- Depending on staff role and environment, it is sometimes necessary and appropriate for them to access systems away from a Solent office base. Where a Solent NHS network is not available, staff can connect to other Wi-Fi networks or use mobile data (3G/4G) and connect via the VPN.

- When working away from the office environment, special care should be taken to ensure that equipment is safe and that sensitive information is not compromised (see appendix 1)

- Staff should also ensure that they are working in a safe and healthy way. Particular care should be taken to ensure that the mobile device is transported safely and used in accordance with Solent DSE (Display Screen Equipment) guidance.

- See appendix 2 for more information on safe use of Mobile computing equipment.

7.1. Working Online

Staff should connect using the Solent VPN and use clinical systems in the same way they would if based in the normal work environment.

7.1.1. Printing via VPN

Normal network printers will be available to print to over the VPN. Follow me printing must be used where possible to protect printed documents. A print job will be saved for 24 hours within the printer queue. No printing should be left on a shared printer unattended.

7.2. Working Offline

7.2.1. Using Clinical Systems

Many clinical systems are not available for use offline. However SystmOne does have a mobile offline version which can be made available to teams with training. SystmOne Mobile downloads a copy of the patient record when connected to the internet. When offline, users can update this offline copy of the record. When re-connected to the network, SystmOne Mobile will sync the local copy of the record into the full patient record.
Any other clinical information should not normally be stored locally on a mobile device. If this is necessary, it will need to be risk assessed and a process agreed with ICT Group and ICT Programme Board to ensure that patient data is kept safe and that the main patient record is kept contemporaneous.

7.2.2. Using non-clinical systems

Non clinical systems that require access to information via the internet cannot be used 'offline'. Staff will need to connect either directly to a Solent network or via the VPN.
Some programs can be used offline, for example, Microsoft Office applications. If used offline, particular care should be taken to ensure that multiple versions of documents are not created and that an offline version of a document is transferred to a Network Drive at the earliest opportunity.

7.3. **Remote Meetings**

Solent Laptops are provided with Microsoft Skype for Business otherwise known as Lync. Lync should, where possible, be used for:

- Instant Messaging
- VOIP calls (internet phone calls)
- Teleconferencing
- Video calls
- Video conferencing
- Sharing documents
- Presenting PowerPoint presentations
- Sharing computer desktop (for remote help and support)

Any or all of these facilities can be used to facilitate remote meetings, including but not limited to: Supervision meetings, Handovers, Team meetings and Training sessions. If Lync is used outside the normal workplace, then particular care should be taken that sensitive or personally identifiable information is not on view or broadcast over speakers.

8. Training Requirements

Basic IT Skills Training is available through the Learning Zone and the Patient Systems Team will support all clinical applications training. Appendix 4

9. Equality Impact Assessment

An Equality Impact Assessment has been carried out assessing this policy (See appendix 3) and no adverse impacts have been found.

10. Monitoring Requirements

The ICT Department routinely audit and monitor relevant aspects of this policy.

11. Policy Review

This policy shall be reviewed every three years or sooner if required.

12. References and Associated Documentation

All references and associated documentation are detailed in the Information Security Policy which can be found on the Trust Intranet.

Appendix 1: Security Procedures Mobile Device

- The device is provided for work purposes on behalf of the Trust and remain the property of the Trust
- The devices are issued to a member of staff to support them to do their job
- If a member of staff leaves the organisation the devices must be returned to the ICT Department
- For security reasons, nobody else should be permitted to use your device, your account names and passwords are not to be divulged to anybody
- The security and use of the device is the responsibility of the member of staff it is assigned to
- In the event that a device is lost or stolen, the member of staff must:
    - Report the theft to the Police and ICT Helpdesk within 24 hours
    - Obtain a Police/Crime/Case number and the name of the investigating officer
    - Complete an Incident Form on the Trust system
- In the event of a member of staff finding their device is not working contact the ICT Helpdesk
- Inappropriate use of the device by an employee will be dealt with under the Disciplinary Policy and Procedure
- The ICT Department will randomly check devices to ensure they are being used in accordance with all Trust policies
- Data usage will be monitored
- The device can be withdrawn at any time on the instructions of the line manager
- The Information Security Policy prohibits the storage of personally identifiable information on the device as the Data Protection Act 1998 requires that personal information remains secure at all times
- Removable media must also be encrypted if used to store confidential information
- Portable devices must be stored securely out of sight overnight, both in the office or if used at home. Portable devices can be left on desks overnight if they are in a secure Solent office/location.

Appendix 2: Portable DSE (Display Screen Equipment) safe use guidance

The Trust will provide training materials to cover the following to help minimise the risks of using portable equipment, including:

- the risks from DSE work and the controls the Trust has put in place
- how to adjust furniture
- how to organise the workplace to avoid awkward or frequently repeated stretching movements
- how to minimise the risk of injury while using portable display equipment:
- Stretch and change position.
- Look into the distance from time to time, and blink often.
- Change activity before users get tired, rather than to recover.
- Short, frequent breaks are better than longer, infrequent ones.
- how to clean the screen and mouse
- who to contact for help and to report problems or symptoms;

Supporting Documents from HSE

Display Screen Equipment Checklist
http://www.hse.gov.uk/pubns/ck1.pdf

Working with display screen equipment (DSE)
http://www.hse.gov.uk/pubns/indg36.pdf

Appendix 3: Equality Impact Assessment

Step 1 – Scoping; identify the policies aims	**Answer**		
1. What are the main aims and objectives of the document?	To provide an appropriate governance framework for mobile working		
2. Who will be affected by it?	This policy applies to all Trust employees, governors, volunteers and contractors.		
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	No existing performance indicators/measures. Outcome is to enable the workforce to be mobile and flexible		
4. What information do you already have on the equality impact of this document?	None this is a new policy		
5. Are there demographic changes or trends locally to be considered?	None		
6. What other information do you need?	None		
Step 2 - Assessing the Impact; consider the data and research	**Yes**	**No**	**Answer** (Evidence)
1. Could the document differentiate unlawfully against any group?		No	Inclusive approach to all mobile working
2. Can any group benefit or be excluded?		No	This policy is aimed at all employees within the organisation and specific requirements can be met in line with UH referrals and recommendations.
3. Can any group be denied fair & equal access to or treatment as a result of this document?		No	This policy is aimed at all employees within the organisation
4. Can this actively promote good relations with and between different groups?	Yes		Actively promotes collaborative mobile working
5. Have you carried out any consultation internally/externally with relevant individual groups?	Yes		Presented at the Working Differently Board and approved.
6. Have you used a variety of different methods of consultation/involvement		No	Policy to be presented to Policy Steering group
Mental Capacity Act implications			
7. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)		No	
External considerations			
8. What external factors have been considered in the development of this policy?			Non Solent staff using Solent kit
9. Are there any external implications in relation to this policy?		No	
10. Which external groups may be affected positively or adversely as a consequence of this policy being implemented?			All groups will be positively impacted by this policy.

Appendix 4: Training Requirements

The ICT Learning Zone has a range of quick reference guides and video to assist staff in basic IT skills training. The ICT Learning Zone can be found on the intranet:

http://solent/GeneralInformation/ICT/LearningZone/default.aspx

ICT Learning Zone covers:

- User Migration
- VPN
- Telephones / mobile phones
- Lync
- Office 2010
- Windows 7
- Outlook
- NHSmail 2

The Patient Systems Team will support all clinical applications training – email SolentPatientSystem.Training@solent.nhs.uk

Appendix 5: Solent NHS Trust Security Management Plan

The relevant section relating to the retention of logs is as follows:

Section 9.2.3 Security Event Monitoring

Trust systems managed by CGI log events that have a relevance to potential breaches of security. The minimum retention period for all Event Logs is one year. Events logged include (where appropriate):

- log-on attempts - recording User IDs, dates and times, successes/failures of attempts;
- creation, amendment and deletion of data - recording User IDs, dates and times;
- access and use of IT all resources including but not limited to internet and Email usage.

For the full policy please see the CGI Security Management Plan v1.2.