The Management of Mobile Devices Policy

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	**The management of mobile devices from mobile phones and laptops through to USB sticks.**
Document Type	X Policy
Reference Number	Solent NHST/Policy/IT02
Version	Version 3
Name of Approving Committees/Groups	Policy Steering Group, Clinical Executive Group
Operational Date	May 2019
Document Review Date	May 2022
Document Sponsor (Job Title)	Director of IT
Document Manager (Job Title)	ICT Technical Assurance Specialist/ ICT Service Manager
Document developed in consultation with	Director of IT, IG Lead, service Engagement, Policy Steering Group
Intranet Location	Business Zone > Policies, SOPs and Clinical Guidelines
Website Location	FOI Publication Scheme
Keywords (for website/intranet uploading)	Mobile Device, Laptop, phone, Policy, IT02

Amendments Summary:

Please fill the table below:

Amend No	Issued	Page	Subject	Action Date
V1	09/05/2019	All	Amendments following group review	
V1.1	03/01/2020	6, item 5.4	Addition of sentence – relating to not leaving devices in cars overnight	
V2	April 2020	6, item 4.15	Addition of sentence – paragraph 4.15 added to include data cap	April 2020
V3	March 2021	4, item 1 and 7, item 10.1 6, item 4.15 6, item 4.15 (new)	Remove reference of asset transfers Remove section relating to data caps Additional section relating to taking devices abroad	March 2021

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes

Contents

1. SUMMARY

The aim of the document is to provide Solent NHS staff with an overview of the lifecycle of a mobile device which could be a mobile phone, tablet, laptop or USB device. The process starts with a Service Request to order the device and ends with a Service Request to return the device.

The management of the device details information on how to manage and maintain your device and expectations on the user regarding how to use and store kit.

2. INTRODUCTION & PURPOSE

2.1 The purpose of this policy is to ensure the secure and responsible use of mobile computing resources of the Trust. This takes the user from making a request for a device through to returning the device on leaving the organisation or no longer requiring the kit.

2.2 The Trust is committed to the provision of a service that is fair accessible and meets the needs of all individuals.

2.3 Mobile devices, such as laptops, smartphones and tablet computers, are important tools which help to enable our staff deliver the expected care our patients require.

2.4 Mobile devices represent a significant risk to information security and data security. If the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to loss of electronic data and malicious software being introduced to our computer network e.g. virus'

2.5 Solent NHS Trust is committed to protecting its information assets in order to safeguard its stakeholders and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

2.6 This policy should be read in conjunction with the Data Protection Compliance Policy

3. SCOPE & DEFINITIONS

3.1 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.

Solent NHS Trust is committed to the principles of Equality and Diversity and will strive to eliminate unlawful discrimination in all its forms. We will strive towards demonstrating fairness and Equal Opportunities for users of services, carers, the wider community and our staff

3.2 Devices covered, but not limited to include:

- Laptops
- Tablets (IPad, Android)
- Mobile phones/Smart Phones
- USB Memory Sticks
- External Storage devices e.g. hard drives, tape drives
- Removable media e.g. DVDs and Blu-Ray disks, as well as diskettes and USB drives

4. PROCESS/REQUIREMENTS

4.1 To request a mobile device (with the exception of mobile phones), staff, or their line manager will need to complete a Service Request via the Self Service Portal. The 'New starter' form can be used for new staff or 'Log a Service Request' for staff already working at the Trust. It is important to note that at least 10 working days needs to be allowed for new starters and 20 working days for all other requests. When staff leave, or no longer need a device a 'Leaver Request' needs to be submitted.

4.2 If staff require specialised ICT kit to support occupational health then a referral is required by the user or the line manager to Occupational Health. Occupational Health hold a selection of regularly requested stock items which can be trialled prior to purchasing.

4.3 To request a mobile phone, users can make requests via SolNet

4.4 Mobile Devices deployed to a service will be the responsibility of the user who will be asked to sign for the device. The service will be responsible for holding the user to account. In the event of misuse or loss, costs will be cross charged to the service responsible for the device.

4.5 It is the responsibility of the user the mobile device is allocated to, to make sure they are used correctly and also returned to IT when they are no longer required along with their power cables/cases when the assigned user leaves the Trust. In the event that a device is not returned to the Trust when the user leaves the Trust, goes on maternity leave or a secondment, the service is responsible for recovering the device or will be charged with the device treated as lost.

4.6 Line Managers with staff returning from maternity/paternity leave, will need to submit the request for devices to be returned to the user. It is important to note that devices cannot be supplied for staff returning for KIT days. These requests will be declined unless the staff member is returning to work within a month of their first KIT day. Line Managers need to be aware that appropriate access of desktop needs to be thought through prior to the staff member returning.

4.7 Un-used mobile devices will be returned to the IT department along with their power cables/cases and not held by the service unless there is a clear and definite business case to do so. This will need to be approved by the Director of IT.

4.8 Laptops and other devices that have **NOT** been connected to the Trust's network for one month will be removed from the domain and will need a Service Request form to be provided to IT to be reactivated or the Laptop/Device will need to be returned to IT.

4.9 Mobile Devices that are not logged onto the Solent IT infrastructure within one month will be considered lost; the cost of replacement (up to £1200) will be the responsibility of the service and will require an incident to be raised.

4.10 Mobile devices that are provided to bank or temporary staff at the request of the service will be the responsibility of the service line manager to obtain when the staff member leaves the Trust. If these devices are not returned they will be reported as stolen to CGI and the Solent ICT team, and the service will be cross charged for replacement. The Service will be expected to raise an incident report and counter fraud will be notified.

4.11 Staff are responsible for ensuring that laptops, even when protected by disk encryption, should not be accessible at any other time to any other individual.

4.12 Mobile Devices are provided to staff to support Trust activities only and must not be used for personal or recreational purposes or by non-authorised staff who do not work for Solent NHS Trust e.g. consultants or council staff. Authorised staff could be users that are on secondment from another Trust or are working on a specific piece of work for a set period of time. Authorisation would be agreed at Senior Management level and clarification over access to systems would need to be cleared with Information governance.

4.13 Staff must ensure that Laptops are connected to the Trust's network at least once a month; this allows for Anti-Virus and security updates to be applied. Devices will still receive updates when connected via VPN but connecting to the network at least once a month is preferred.

4.14 The Trust does not support the use of in car chargers for charging up laptops. There is a risk of fire and therefore the Trust will decline all requests to purchase chargers and will not support the use of personally owned chargers. Issues with battery life need to be referred to the service desk who will investigate.

4.15 If you need to take your laptop or mobile phone abroad, written permission by Solent ICT is required in all instances. Please make a written request to ICTPMO@solent.nhs.uk. If agreed, once abroad, devices must only be connected to secure WiFi to avoid data roaming charges.

5. PHYSICAL SECURITY

5.1 Mobile Devices should be 'screen locked' and only be left in a secure location i.e. Solent office or protected office during working hours. Devices should not be left overnight on desks and should be taken home or placed in lockers.

5.2 All removable media such as CD-ROM and USB Memory sticks should be removed unless absolutely necessary.

5.3 Ensure that Mobile Devices are not left unattended when working off-site

5.4 When travelling and not in use, ensure that Mobile Devices are stored securely out of sight. For example, when travelling by car, ensure laptops are locked in the boot. Devices left on display and unattended will inevitably attract attention and are likely to be stolen. This will be treated as a breach of IG and an incident will be logged with appropriate action taken.

It is important that mobile devices are not left in car boots overnight, even on driveways.

6. INCIDENT REPORTING

6.1 Loss of Trust Mobile Devices must be reported to the IT Service Desk immediately so that the account can be disabled. An incident will then need to be logged and appropriate action taken.

7. ROLES & RESPONSIBILITIES

7.1 All Solent NHS Trust staff will have an awareness of Data Protection Compliance Policy.

Solent Director of IT – Oversight and management of overall IT service
CGI Director of IT – Oversight and management of overall IT service delivered to Solent NHS Trust
Solent Service Manager – Day to day and operational management of IT services and first line of contact with third party contractor
CGI Service Manager - Day to day and operational management of IT services delivered to Solent NHS Trust including asset management (hardware and licence management)

8. TRAINING

8.1 All staff must complete annual mandatory training on Information Governance which will cover use of mobile data and devices.

9. EQUALITY IMPACT ASSESSMENT AND MENTAL CAPACITY

This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

10. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

10.1 The criteria for success is that all devices will be returned to the Trust if not in use for more than one month.

Staff must be aware of their responsibility to look after their Trust devices and therefore the number of stolen or mislaid devices will be reduced.

10.2 The data will be provided and reviewed on a monthly basis by the ICT team and reported at ICT Committee and IT Security Group. The team will work with the Service Engagement team to educate services as to the importance and benefits of adhering to this policy.

Where devices are not returned, or are mislaid, this will be brought to the attention of the Service Managers who will be responsible for recovering devices or covering the costs.

11. REVIEW

11.1 This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed 1 year from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

12. REFERENCES AND LINKS TO OTHER DOCUMENTS

12.1 Information on ICT policies can be accessed on SolNet.

Appendix: A Equality Impact Assessment

Step 1 – Scoping; identify the policies aims	**Answer**		
1. What are the main aims and objectives of the document?	To provide Solent staff with clear principles and standards to adhere to when using mobile devices		
2. Who will be affected by it?	Solent Staff		
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	Compliance with Data Protection Legislation and the secure handling of mobile devices and the data held within them		
4. What information do you already have on the equality impact of this document?	None		
5. Are there demographic changes or trends locally to be considered?	No		
6. What other information do you need?	N/A		
Step 2 - Assessing the Impact; consider the data and research	**Yes**	**No**	**Answer** (Evidence)
1. Could the document unlawfully discriminate against any group?		X	
2. Can any group benefit or be excluded?		X	
3. Can any group be denied fair & equal access to, or, treatment as a result of this document?		X	
4. Can this actively promote good relations with and between different groups?	X		Mobile working
5. Have you carried out any consultation internally/externally with relevant individual groups?	X		ICT Senior Leads, Data Protection Review, ICT Committee
6. Have you used a variety of different methods of consultation/involvement?	X		Email consultation and group discussions
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)		X	

External considerations			
8. What external factors have been considered in the development of this policy?			Relationships with third parties i.e. ICT Contractors and non-Solent staff that work and use Solent kit. This includes rotating doctors and students. How data is managed in line with national IG guidelines.
9. Are there any external implications in relation to this policy?			Not all non-Solent staff who work on Solent sites would be legible for kit based on the revised policy.
10. Which external groups may be affected positively or adversely as a consequence of this policy being implemented?			Non-Solent staff that work and use Solent kit. This includes rotating doctors and students. However, this has been discussed with relevant teams and has not to date had a negative impact. Each request is reviewed on a 'case by case' basis.