
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	<input checked="" type="checkbox"/> Policy
Reference Number	Solent NHST/Policy/IT02
Version	Version 4
Name of Approving Committees/Groups	Policy Steering Group, Clinical Executive Group
Operational Date	April 2022
Document Review Date	April 2025
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
V4	March 2022	6.1 4.13 4.8 7.1 12.1	Expansion of police reporting policy. Length of time to update devices with security patching. Change to downed asset policy. Expansion of compliance policy. Reference to DSE and Mobile Device Policy.	March 2022

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes
4	March 2022	Leigh Metzelaar	Policy Steering Group, Clinical Executive Group	Standard 3-year review

Contents

.....	1
1. SUMMARY.....	4
2. INTRODUCTION & PURPOSE.....	4
3. SCOPE & DEFINITIONS.....	4
4. PROCESS/REQUIREMENTS.....	5
5. PHYSICAL SECURITY.....	6
6. INCIDENT REPORTING.....	7
7. ROLES & RESPONSIBILITIES.....	7
8. TRAINING.....	7
9. EQUALITY IMPACT ASSESSMENT AND MENTAL CAPACITY.....	7
10. SUCCESS CRITERIA / MONITORING EFFECTIVENESS.....	7
11. REVIEW.....	8
12. REFERENCES AND LINKS TO OTHER DOCUMENTS.....	8

The Management of Mobile Devices Policy

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, as an example 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 and Patient Safety Partners), 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 MYIT 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 returned to IT when they are no longer required along with their power cables/cases, when the assigned user leaves the Trust. If 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 Keep In Touch (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 eight weeks will be removed from the domain and will need a Service Request to renew. If the device has been downed in three weeks the user may reactivate via the ICT helpdesk. If over eight weeks the Laptop/Device will need to be returned to IT with appropriate service request and renewed. The current policy is to down the device after three weeks.
- 4.9 Mobile Devices that are not logged onto the Solent IT infrastructure within eight weeks will be considered lost; the cost of replacement (up to £1200) will be the responsibility of the service and will require an incident report to be completed.
- 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 missing 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-authorized staff who do not work for Solent NHS Trust. 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 every two weeks; 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 weekly is preferred. The device should be connected for at least two hours to allow for updates.
- 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 Wi-Fi 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 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. 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. A police report should also be sought with appropriate police reference number. An incident report will then need to be completed and appropriate action taken.

7. ROLES & RESPONSIBILITIES

- 7.1 **All Solent NHS Trust staff** will have an awareness and comply with the 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 criterion 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.
Please refer to 'Use of Display Screen Equipment and Mobile Devices Policy'.

Appendix: A Equality Impact Assessment

Equality Analysis is a way of considering the potential impact on different groups protected from discrimination by the Equality Act 2010. It is a legal requirement that places a duty on public sector organisations (The Public Sector Equality Duty) to integrate consideration of Equality, Diversity and Inclusion into their day-to-day business. The Equality Duty has 3 aims, it requires public bodies to have due regard to the need to:

- **eliminate unlawful discrimination**, harassment, victimisation and other conduct prohibited by the Equality Act of 2010;
- **advance equality of opportunity** between people who share a protected characteristic and people who do not;
- **foster good relations** between people who share a protected characteristic and people who do not.

Equality Impact Assessment (EIA) is a tool for examining the main functions and policies of an organisation to see whether they have the potential to affect people differently. Their purpose is to identify and address existing or potential inequalities, resulting from policy and practice development. Ideally, EIAs should cover all the strands of diversity and Inclusion. It will help us better understand its functions and the way decisions are made by:

- **considering the current situation**
- **deciding the aims and intended outcomes of a function or policy**
- **considering what evidence there is to support the decision and identifying any gaps**
- **ensuring it is an informed decision**

You can find further information via the e-learning module [here](#) [insert updated link once finalised]

Equality Impact Assessment (EIA)

Step 1: Scoping and Identifying the Aims

Service Line / Department	ICT	
Title of Change:	Management of Mobile Devices Policy	
What are you completing this EIA for? (Please select):	Policy	<i>(If other please specify here)</i>
What are the main aims / objectives of the changes.	Update to Policy	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below. If there is no impact, please select "not applicable":

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Not applicable	Action to address negative impact: <i>(e.g. adjustment to the policy)</i>
Sex			NA	
Gender reassignment			NA	
Disability			NA	

Age			NA	
Sexual Orientation			NA	
Pregnancy and maternity			NA	
Marriage and civil partnership			NA	
Religion or belief			NA	
Race			NA	

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?)	No	Policy for staff members.
Have you taken into consideration any regulations, professional standards?	No	Standard organisational practices and measures.

Step 3: Review, Risk and Action Plans

How would you rate the overall level of impact / risk to the organisation if no action taken?	Low	Medium	High
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
What action needs to be taken to reduce or eliminate the negative impact?	N/A		
Who will be responsible for monitoring and regular review of the document / policy?	N/A		

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	L Metzelaar	Date:	12.04.2022
--------------------	-------------	-------	------------

Additional guidance

Protected characteristic	Who to Consider	Example issues to consider	Further guidance
1. Disability	A person has a disability if they have a physical or mental impairment which has a substantial and long term effect on that person's ability to carry out normal day today activities. Includes mobility, sight, speech and language, mental health, HIV, multiple sclerosis, cancer	<ul style="list-style-type: none"> • Accessibility • Communication formats (visual & auditory) • Reasonable adjustments. • Vulnerable to harassment and hate crime. 	Further guidance can be sought from: Solent Disability Resource Group
2. Sex	A man or woman	<ul style="list-style-type: none"> • Caring responsibilities • Domestic Violence • Equal pay • Under (over) representation 	Further guidance can be sought from: Solent HR Team
3 Race	Refers to an individual or group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.	<ul style="list-style-type: none"> • Communication • Language • Cultural traditions • Customs • Harassment and hate crime • "Romany Gypsies and Irish Travellers", are protected from discrimination under the 'Race' protected characteristic 	Further guidance can be sought from: BAME Resource Group
4 Age	Refers to a person belonging to a particular age range of ages (eg, 18-30 year olds) Equality Act legislation defines age as 18 years and above	<ul style="list-style-type: none"> • Assumptions based on the age range • Capabilities & experience • Access to services technology skills/knowledge 	Further guidance can be sought from: Solent HR Team
5 Gender Reassignment	" The expression of gender characteristics that are not stereotypically associated with ones sex at birth" World Professional Association Transgender Health 2011	<ul style="list-style-type: none"> • Tran's people should be accommodated according to their presentation, the way they dress, the name or pronouns that they currently use. 	Further guidance can be sought from: Solent LGBT+ Resource Group
6 Sexual Orientation	Whether a person's attraction is towards their own sex, the opposite sex or both sexes.	<ul style="list-style-type: none"> • Lifestyle • Family • Partners • Vulnerable to harassment and hate crime 	Further guidance can be sought from: Solent LGBT+ Resource Group
7 Religion and/or belief	Religion has the meaning usually given to it but belief includes religious and philosophical beliefs, including lack of belief (e.g Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition. (Excludes political beliefs)	<ul style="list-style-type: none"> • Disrespect and lack of awareness • Religious significance dates/events • Space for worship or reflection 	Further guidance can be sought from: Solent Multi-Faith Resource Group Solent Chaplain
8 Marriage	Marriage has the same effect in relation to same sex couples as it has in relation to opposite sex couples under English law.	<ul style="list-style-type: none"> • Pensions • Childcare • Flexible working • Adoption leave 	Further guidance can be sought from: Solent HR Team
9 Pregnancy and Maternity	Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In non-work context, protection against maternity discrimination is for 26 weeks after giving birth.	<ul style="list-style-type: none"> • Employment rights during pregnancy and post pregnancy • Treating a woman unfavourably because she is breastfeeding • Childcare responsibilities • Flexibility 	Further guidance can be sought from: Solent HR team