Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

MOBILE DEVICE USER POLICY

POLICY

Reference	E&F 002		
Approving Body	*Estates and Facilities Governance Group*		
Date Approved	*3 February 2022*		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
	yes		
Issue Date	*February 2022*		
Version	*Version 2*		
Summary of Changes from Previous Version	*Update to new Policy template*		
Supersedes	*Version 1*		
Document Category	*Estates & Facilities*		
Consultation Undertaken	*Mobile Device Group*		
Date of Completion of Equality Impact Assessment	*03/02/22*		
Date of Environmental Impact Assessment (if applicable)	*N/A*		
Legal and/or Accreditation Implications	*Data Protection Act 2018* *The Computer Misuse Act 1990*		
Target Audience	*All Trust staff that are required to loan and use a Trust mobile device for their job role*		
Review Date	*February 2025* **EXTENDED TO 30th September 2026**		
Sponsor (Position)	*Associate Director of Estates & Facilities*		
Author (Position & Name)	*Clinical Lead for ICT*		
Lead Division/ Directorate	*Corporate Division*		
Lead Specialty/ Service/ Department	*Clinical Digital Services*		
Position of Person able to provide Further Guidance/Information	*Nervecentre System Manager*		

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
N/A	*N/A*

CONTENTS

Item	Title	Page
1.0	INTRODUCTION	3
2.0	POLICY STATEMENT	3
3.0	DEFINITIONS/ ABBREVIATIONS	3
4.0	ROLES AND RESPONSIBILITIES	4
5.0	APPROVAL	4
6.0	DOCUMENT REQUIREMENTS	4
6.1	Mobile Device Issue	4
6.2	Physical Protection and Maintenance	5
6.3	Lost or Stolen Devices	6
6.4	Software Updates	8
6.5	Personal Use of Mobile Devices	8
6.6	Returning of Mobile Devices	8
7.0	MONITORING COMPLIANCE AND EFFECTIVENESS	9
8.0	TRAINING AND IMPLEMENTATION	10
9.0	IMPACT ASSESSMENTS	10
10.0	EVIDENCE BASE (Relevant Legislation/ National Guidance) and RELATED SFHFT DOCUMENTS	10
11.0	APPENDICES	10

APPENDICIES

Appendix 1	*Equality Impact Assessment form (EQIA)*	11
Appendix 2	*Environment Impact Assessment*	13
Appendix 3	*Device Decision Algorithm*	14
Appendix 4	*Example of Mobile Device Asset Signature Sheet Receipt*	15
Appendix 5	*Actions to be taken by individuals and issuing authority to trace and rec over any lost or stolen device*	16

1.0 INTRODUCTION

As part of the major digital transformation project Sherwood Forest Hospitals NHS Foundation Trust (Trust) recognises the advantages in the utilisation of mobile devices for staff during the performance of their duties.

2.0 POLICY STATEMENT

The purpose of this Policy is to describe in detail the arrangements for the correct management, issue and disposal of mobile devices in order to:

- Direct all staff in their roles and responsibilities in the use of and receiving of loaned mobile devices.
- Ensure good practice in protection of patient confidentiality and identity.
- Prevent misuse of any mobile devices that may result in complaints or legal proceedings.
- Ensure that all mobile devices are managed safely and legally.
- To ensure the appropriate loaned device is allocated as agreed by the Trust to ensure the allocation of devices and subsequent management is standardised.
- To ensure access and use of mobile devices is authorised and managed.
- To ensure there is clear oversight of relevant equipment.

This policy applies to all personally loaned Trust mobile devices capable of storing data and connecting to a network. This includes, but is not limited all devices and accompanying media that fit the following classifications:

iPhone
iPod
Laptop
MacBook
Notebook
iPads
Smartphone
Tablet
Excludes –Vocera, Bleeps

3.0 DEFINITIONS/ ABBREVIATIONS

- AD – Active Directory.
- AirWatch – Software security and management suite.
- User - Any authorised individual using Trust systems as a trainee, student, contractor, volunteer or otherwise on Trust business.
- Baton Device - generic use devices held by each ward/ operational area for use by non-permanent staffs.
- BYOD – Bring your own device.
- Nervecentre – Database management system.
- NHIS - Nottinghamshire Healthcare Informatics Service.

- NHIS issued devices – Mobile phones, laptops/notebook computers.
- PCDID – Personal confidential data.
- Trust - Sherwood Forest Hospitals NHS Foundation Trust.
- User ID – a username.

4.0 ROLES AND RESPONSIBILITIES

4.1. The User in receipt of a Trust mobile device, including contract and temporary workers, are responsible to act in accordance with associated Trust policies and procedures.

4.2 Line Manager or Head of Department has to approve and authorise a user to have access to a mobile device (See HR new starter process).

4.2 NHIS are responsible for asset control management and issuing mobile devices that are not Nervecentre devices.

They are responsible for the accreditation of each user AD Account, including Nervecentre, to the correct user groups within AirWatch to enable the user to be imported into patient data systems where applicable.

4.3 The Nervecentre System Manager is responsible for asset control management and issuing Nervecentre devices. The importation of user accredited AD Accounts into the Nervecentre Database System.

5.0 APPROVAL

Group/Individual/Consultation	Date	Comments	Approved
Mobile Device Working group	31 Oct 2018	Nil	Yes
Cyber Security Group			
Divisional Governance Leads			
HR	20 Nov 2018	Nil	Yes
JSPF	20 Nov 2018	Nil	Yes
Staff Comms and Engagement Forum			

6.0 DOCUMENT REQUIREMENTS

6.1 Mobile Device Issue

Mobile devices should be issued dependant on the connectivity and or clinical requirements of the individual job role. For further detail see The Device Decision Algorithm (Appendix 3) assesses which device meets an individual's requirement for their role.

Temporary staff will not usually be issued a device. However ward/work area Baton Devices, Locum Baton phones (held by Hospital Out of Hours (HOOH) Team) or Trust desktop computers will be available for use. Where in the unlikely event exceptions are identified, these will be

managed on an individual basis by the line manager in conjunction with NHIS and the Nervecentre System Manager.

We do not currently run a BYOD programme.

All staff are responsible for ensuring mobile devices are kept safe and only used for the business it is intended for, as detailed in associated Trust Polices and National Legislation.
All mobile devices issued by the organisation are issued to a named individual only and must not be shared or used by anyone who is not recorded as the asset owner, this for audit purposes and to comply with the Data Protection Act 1998.

A user can only receive a device once it has been approved by a manager and their AD Account has been accredited correctly to allow them to access authorised patient data management systems and other applications.

Each user signs a receipt for their loaned device, which includes the mandatory device case and accessories (charger plug, cable, etc) on a Mobile Device Asset Signature Sheet receipt (Appendix 4).

Each device will have a Trust Security and Access Code applied to it on blue and white Asset stickers. Users are not to interfere with or remove the NHIS Asset sticker.

6.2 Physical Protection and Maintenance

Staff are personally responsible for the security of the mobile device at all times whether this is on Trust premises, the premises of other organisations, in the car, on public transport or at home. All devices must carry the standard NHIS asset register number.

Care should be taken when using mobile devices in public places, particularly regarding password security and ensuring that screens cannot be overlooked; particularly if they contain personal confidential data.

To best safeguard your loaned Trust device, users should:

a. Always keep the device safe, on your person or locked in a secure location.
b. Never loan your device to another user under any circumstance.
c. Meet infection control requirements and clean the device case regularly using Clinell wipes.

Devices issued with a Trust standard case must be kept in it, in order to:

d. Easily identify the device as a Trust device and not as a personal device being accessed in the workplace.
e. Minimise accidental damage.

Any faults and or damage should be reported to NHIS on extension 4040 and a call logged to have the device inspected and rectified.

6.3 Lost or Stolen Devices (See Flow Chart)

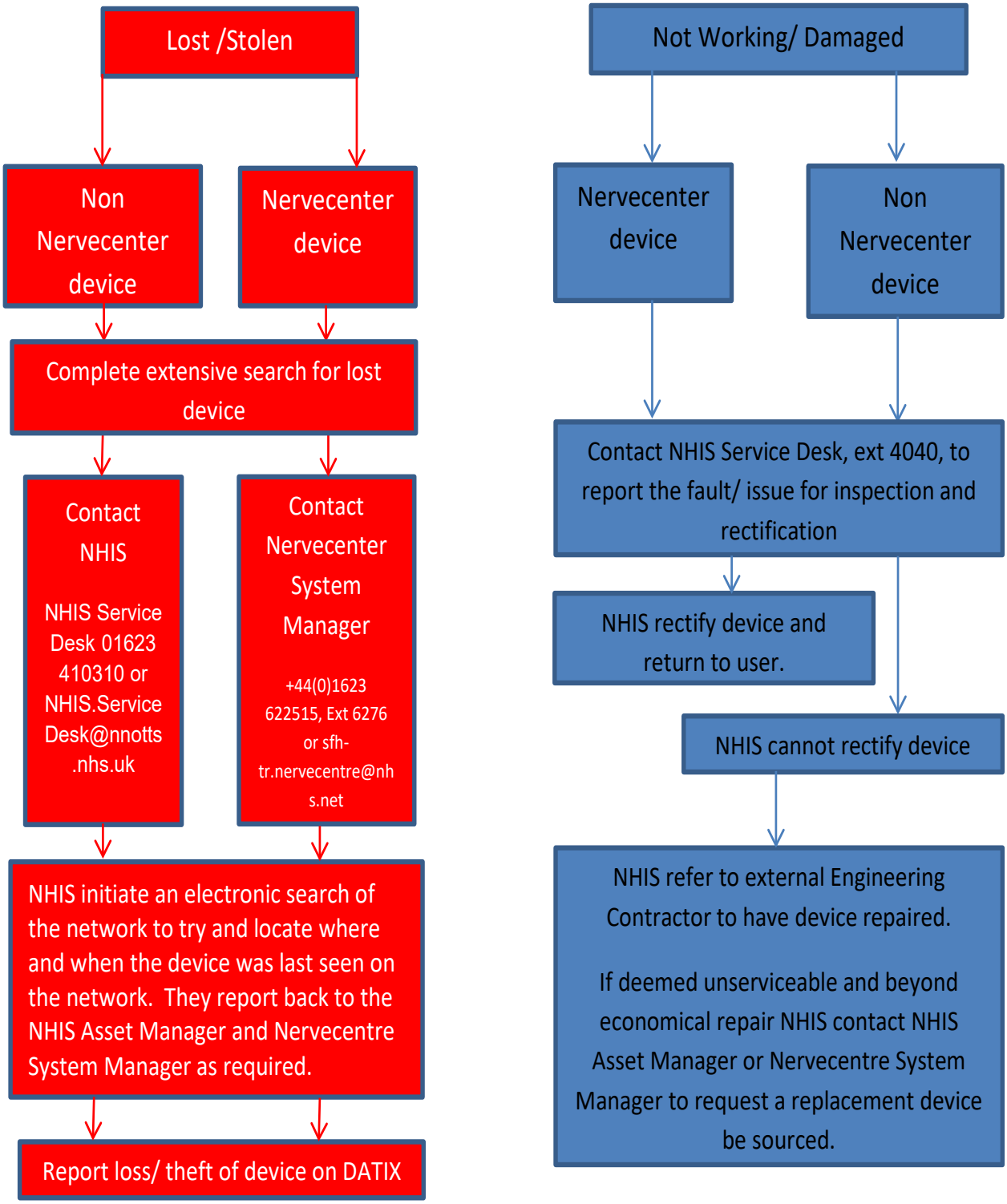
It is important that any device that is presumed to be lost, after an extensive search has been completed, or has been stolen is reported to individual Line Managers and to the Issuing Authority (NHIS Device Manager or Nervecentre System Manager as appropriate) as soon as is practicably possible. All lost or stolen mobile devices will be investigated and recovery action instigated, if possible. If the replacement of a lost or stolen device is deemed to be urgently required, it will be replaced; though this will be negotiated on a case by case basis and may be in the form of a temporary device until a permanent replacement solution can be sourced.

Appendix 5 gives more detail of steps to be taken by individuals to trace, report and recover any lost or stolen devices. It also details the reporting, electronic tracing and support actions that the Issuing Authority will carry out to try to find and manage the device, after the loss or theft.

Any loss of mobile devices are to be reported on DATIX in accordance with the Trust's information governance incident reporting policy, quoting the Police crime number if applicable.

If the device is known to have been stolen, i.e. taken during a burglary, then the theft is to be reported to the appropriate line manager and the Police, the Crime Number is to be recorded as part of the loss reporting process.

Device Management



6.4 Software Updates

Mobile device operating system updates are released periodically throughout the year. These have to be tested and assured prior to installation to ensure compatibility with patient data management system applications. When these are received on the device, the updates should not be accepted until NHIS and the Nervecentre System Manager advise it is safe to do so via an internal communications notification.

6.5 Personal use of mobile devices

Mobile devices are supplied to staff for business use and users should not attempt to load their own software, including games and screensavers. As per Email and Internet Policy.
The Trust acknowledges staff can access their emails at home or when not on duty and should they wish to do this, it is their preference and not an expectation.

6.6 Returning of Mobile Devices

Upon leaving the organisation or when required all loaned mobile devices must be handed back to the Trust with their device case and accessories (charger plug, cable, etc).
Failure to return the mobile device at the end of your employment may result in legal action being taken against you to recover the item value.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Adherence to the Mobile Device Policy	Line Manager	Review any associated IG breaches associated with Trust mobile devices	As notified by incidents	
Asset Register	NHIS	Review of loaned devices against users	Annually	
Mobile phone usage/bills	Relevant budget holder	Divisional budget against spend	Monthly	

8.0 TRAINING AND IMPLEMENTATION

All staff agree this is a loaned device and understand the content of the policy before accepting and signing.
All staff receiving mobile devices will receive training in the use of their mobile device including:

- its security functionality
- responsibility for safeguarding the device
- obligation to comply with Information Governance

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1.
- This document has been subject to an Environmental Impact Assessment, see completed form at Appendix 2.

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- The Computer Misuse Act 1990
- Data Protection Act 1998
- Information Governance

Related SFHFT Documents:

- Electronic Remote Working Policy
- Guidance for Asset Owners and Information Asset Administrators
- Information Security Policy
- Equality and Diversity Policy
- Data Protection, Confidentiality and Disclosure Policy
- Information Security Policy
- Internet and Email Policy
- Social Media Policy
- Photography and Video Recording Policy
- Information Governance Policy
- NHIS Corporate Mobile Device Acceptable Use Policy
- SFH Counter Fraud and Corruption Policy

11.0 APPENDICES

- Appendix 1 Equality Impact Assessment
- Appendix 2 Environmental Impact Assessment
- Appendix 3 Device Decision Algorithm
- Appendix 4 Example of Mobile Device Asset Signature Sheet receipt
- Appendix 5 Actions to be taken by Individuals and Issuing Authority to trace and recover any lost or stolen device

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Mobile Device Policy			
New or existing service/policy/procedure: existing			
Date of Assessment: February 2022			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	None		
Gender	None		
Age	None		
Religion	None		
Disability	Yes	• Employees to the Trust declare any disability at time of job application for further assessment and adjustment on an individual basis • Adjust settings to meet individual needs e.g. Device text can be increased • Use of voice command is available • Access to Work Resources	

		• Previous risk assessment undertaken as part of Nerve Centre project initiation and closed	
Sexuality	None		
Pregnancy and Maternity	None		
Gender Reassignment	None		
Marriage and Civil Partnership	None		
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None		

What consultation with protected characteristic groups including patient groups have you carried out?
N/A

What data or information did you use in support of this EqIA?
- Equality and Diversity Policy

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?
No

Level of impact

From the information provided above and following EQIA guidance document Guidance on how to complete an EIA (click here), please indicate the perceived level of impact:
Low Level of Impact
For high or medium levels of impact, please forward a copy of this form to the HR Secretaries for inclusion at the next Diversity and Inclusivity meeting.

Name of Responsible Person undertaking this assessment:
Clinical Lead for ICT

Signature:

Date: 16/02/22

APPENDIX 2 – ENVIRONMENTAL IMPACT ASSESSMENT

The purpose of an environmental impact assessment is to identify the environmental impact, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	Environmental Risk/Impacts to consider	Yes/No	Action Taken (where necessary)
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	No	
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released? (e.g. lubricants, liquid chemicals) • Does the policy fail to consider the need to provide adequate containment for these substances? (For example bunded containers, etc.)	No	
Water	• Is the policy likely to result in an increase of water usage? (estimate quantities) • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water) • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	No	
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (For example use of a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.) • Does the policy fail to include a procedure to mitigate the effects? • Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	No	
Energy	• Does the policy result in an increase in energy consumption levels in the Trust? (estimate quantities)	No	The policy does not recognise the number of devices, as the devices already in use pre-policy; this

			would not increase the current energy usage.
Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	No	

Appendix 3 Device Decision Algorithm

See attached (A3) – Device Decision Algorithm Pre-procurement

E&F 002.1 Appendix 3 - Mobile Device Dec

Appendix 4 Example of Mobile Device Asset Signature Sheet receipt

NHS Sherwood Forest Hospitals NHS Foundation Trust

Mobile Device Asset Signature Sheet — Location

Sherwood Forest Hospitals NHS Foundation Trust policy says that loaned mobile devices are correctly registered on the holder's inventory, is serviceable for its intended purpose and is traceable at all times. Loans made to individuals of Clinical Digital Platform devices are to be recorded on the Mobile Device Asset Signature Sheet, are to be agreed to by the borrower and the form kept by the inventory holder. All borrowers are to abide by the loan conditions as detailed within the 'Borrower Declaration' detailed below.

Borrower Declaration

I understand that it is my responsibility to look after and safeguard the aforementioned Trust device and ancillary equipment (charger plug, lead, headphones, case & box), that I will only utilise it for its intended purpose for the operation of the preloaded clinical digital applications, my personal NHS email account and the associated preloaded apps and links. I further understand that I will not remove the approved Trust apps or weblinks from the device. I understand that my personal unlock code, that opens access to all functionality on the idevice, is not to be shared with any other person and I am not to loan my idevice to any other party under any circumstance. I understand that the device (complete as issued) is to be returned to the Mobile Device Manager upon the completion of my assignment, rotation cycle or when requested to do so through early recall.

Number	Device Name	Device Type	Username/ Alias	First Name	Surname	Title/ Role	Specialty/ Location	Device Serial Number	IMEI No (iPhones)	SFHFT Asset No	IOS Version	Mac Address	Unlock Code	Signature
1	iPod Touch - 1	iPod Touch, 16GB, Grey												
2	iPod Touch - 2	iPod Touch, 16GB, Grey												
3	iPone - 1	iPhone 6s, Space Grey, 32GB												
4	iPone - 2	iPhone 6s, Space Grey, 32GB												
5	iPad - 1	iPad, 12.8 GB, Grey												
6	iPad - 2	iPad, 12.8 GB, Grey												

Appendix 5 Actions to be taken by Individuals and Issuing Authority to trace and recover any lost or stolen device

Serial	Lost Device	Stolen Device
1	Upon discovering that your loaned Trust device has been lost, you are to instigate a thorough search of all of your work areas, 'retracing your steps' to all the areas that you know that you took your device into.	Upon discovering that your loaned Trust device has been stolen, such as in a burglary, bag theft, 'phone jacking', etc. You are to report the theft to the Police and obtain a crime number. Do not put yourself in harm's way to recover the device.
2	You are to check with all work colleagues to see if they have inadvertently picked up your device by accident or are safeguarding it on your behalf.	You are to report its theft to your Line Management and you are to inform the Issuing Authority (NHIS Device Manager or Nervecentre System Manager as appropriate). Furnishing them with a copy of the crime number.
3	You are to report its loss to and check with your Line Management to see if they have safeguarded it on your behalf.	The Issuing Authority will immediately initiate the 'wiping' of the device to render it useless and will begin sourcing a replacement device*.
4	If after an extensive search and checking with colleagues and Line Managers your device cannot be found you are to contact the Issuing Authority (NHIS Device Manager or Nervecentre System Manager as appropriate) to report its loss and to request assistance in electronically tracking your device.	The individual is to report the theft on DATIX and copy the DATIX report reference number to the Issuing Authority for the completion of the Loss Register.
5	If the device is located by electronic tracking, circumstances depending, either the location will be passed to the individual for retrieval or the device will be retrieved by the Issuing Authority on their behalf.	
6	If the device cannot be electronically located and all search options have been exhausted then the device will be deemed to be lost. The individual will be informed of this outcome and will be requested to report the loss on DATIX in accordance with the Trust's information governance incident reporting policy. The DATIX report reference number is to be copied to the Issuing Authority for the completion of the Loss Register.	
7	Once a device is deemed to be lost and has been reported on DATIX by the individual loaner, the Issuing Authority will initiate the 'wiping' of the device to render it useless and will begin sourcing of a replacement device*.	

*It is to be noted that replacement devices may differ from the specification of the originally loaned item in both specification and condition. This will depend upon resource availability at the time