Mobile Device Allocation and Usage Policy

Document Author: Infrastructure & Voice Communication Manager

Date Approved: June 2023

Document Reference	ICT - Mobile Device Allocation and Usage
Version	V 4.0
Responsible Committee	ICT Management Group
Responsible Director (title)	Chief Information Officer (CIO)
Document Author (title)	Infrastructure & Voice Communication Manager
Approved By	Trust Management Group
Date Approved	June 2023
Review Date	June 2025
Equality Impact Assessed (EIA)	Not Applicable
Protective Marking	Not Protectively Marked

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
0.1	13/06/2017	Michael C Foster	D	Introductions 1- update term smartphone. Process 2- Mobile phone entitlement. Process 2.3.2 - Monthly contribution to personal bill.
0.2	21/01/2017	Stephanie Appleyard	D	Moved to new template and
0.3	26/06/2017	Michael C Foster	D	Introduce and update version control
0.4	26/06/2017	Ola Zahran	D	Tariff change after discussion with Mark Bradley
1.0	09/08/2017	Michael C Foster	A	Approved by TMG
1.1	Feb 18	Risk Team	D	Document formatted – New visual identity. Addition of section 2.3.6
2.0	Oct 18	ICT	A	Approved at TMG
2.1	Oct 2020	Ruth Parker	D	Date agreed by TMG for review date extension
2.2	Jan 2020	Martin Lane	D	Remove reference to Sup13
2.2	Jan 2020	Helen Hartland	D	Minor change to the IG links
2.3	Jan 2021	Ola Zahran	D	Added reference to tablet and removed BYOD as this will cover in a new policy
3.0	Feb 2021	Risk Team	A	Approved at TMG
3.1	Oct 2021	Risk Team	A	Responsible Director changed to reflect current structure
3.2	Jan 2023	ICT	D	Various amendments – particularly around data usage and personal use.
3.3	March 2023	PDG	D	Approved at PDG
3.4	April 2023	JSG	D	Minimal changes approved in relation to data usage and personal use
4.0	June 2023	Risk Team	A	Approved at TMG
A = Approved D = Draft				
Document Author = Infrastructure & Voice Communication Manager				
Associated Documentation: Insert names of associated Policies or Procedures here				

Staff Summary

Mobile phone entitlement
Supply, usage and care requirements
Trust and mobile user responsibilities
Procedures for making international calls
Call tariffs
Procedure for investigation of potential excessive use

1.0 Introduction

1.1 This policy applies to anyone, including Trust staff, contractors and other NHS staff who have been issued with, or have access to a Trust mobile device.

1.2 The purpose of this policy is to clearly define the responsibilities of both the Trust and the users of mobile devices. This will cover supply, usage and care of all mobile devices.

1.3 Within this document the term 'Smartphone' refers to a mobile device with internet capability, providing access to services such as email. Where a 'Standard phone' is specified, this refers to mobile devices which are voice-only, not enabled for data.

2.0 Process

2.1 Requisitions

2.1.1 Mobile phone or tablet entitlement will be based on the following criteria and should be authorised by AD or head of Department/Sector Commander:

- Mobile Manager/ On call staff – Smartphone and/or tablet
- Frontline mobile staff (Ops, EOC, PTS, IUC) – Smartphone/Standard pho
- Corporate support staff without a fixed work location.
- A staff role with a business requirement for mobile phone or smart phone, a business case is to be provided by line manager and authorisation to be granted by department Head or Associate Director.
- Mobile Support Staff – Smartphone or Standard mobile phone

Any exceptions to the above criteria will need authorisation from an Associate Director or Head of Department.
This includes but not limited to the following:

2.1.2 All mobile devices (standard phone or smartphone or Tablet) must be requested via the ICT Service Desk who will provide a reference number detailing the requirements. The request will be electronically sent to the relevant budget holder who should consider the above criteria before authorising the request.

2.2 Trust Responsibilities

It is the responsibility of the Trust to ensure that where there is a necessary requirement, that an appropriate mobile device is provided.

- The Trust will make the final decision on the make and model of the required device to provide continuity and effective management of cost to the Trust.
- The Trust will monitor the usage of each device to assess ongoing suitability and cost.
- The Trust is responsible for providing upon request via ICT Service Desk an individual's own itemised mobile phone bill to allow users to monitor their own usage.
- The Trust will ensure that all devices have mandatory passwords in place in order to protect the integrity of the data that is stored on the device.

2.3 Mobile User Responsibilities

2.3.1 Mobile Users are responsible for the day-to-day care of the mobile device and should take all necessary precautions to ensure that the device does not become damaged, lost or stolen. All incidents of damage or the loss or theft of a mobile device must be reported using the Datix incident management system or Datix telephone hotline on 0300 330 5419 and then to the ICT Service Desk via the online portal or by telephone 0300 330 5417. Loss or theft should be reported as soon as identified to allow ICT to wipe and or secure the data that may be stored on the device. Theft should also be reported to the police and a crime reference number must be obtained.

NB: At the discretion of the Trust a charge for the full cost of replacement equipment and the cost of any unauthorised calls and/or usage may be levied from the employee e.g. in the event of wilful misuse or failure to take adequate steps to safeguard the device.

2.3.2 All mobile users should be aware that the mobile device that they have been provided with is for use on Trust business. An allowance is made for limited personal use which includes local, national and mobile calls as well as SMS text messages. The use of personal mobile data should be limited and not used excessively. Users should make use of wireless networks to minimise the amount of mobile data used – high bandwidth applications such as video should be avoided when using mobile data. All bills will be monitored by the Trust to ensure that there is no misuse of mobile devices.

2.3.3 Tethering, also known as mobile hotspot, is not to be used on a regular basis and should only be used in an emergency and is not a direct replacement for your home broadband. Many health organisations provide a wireless network which is available to NHS Trust staff called 'govroam', it is allowed on Trust and personal devices and staff can login with their personal YAS credentials.

2.3.4 Staff who are responding or working on behalf of the Trust must ensure that they have access to their issued mobile phone for the duration of their duty.

2.3.5 Mobile users should comply with the Road Traffic Act with regards to usage of their mobile device while driving.

2.3.6 Each mobile user will be expected to sign to agree to compliance with the following counter fraud declaration on receipt of their device:

I agree to the disclosure of mobile device billing information for monitoring and evaluation purposes. In the event of inappropriate usage or fraudulent applications I am aware it is a disciplinary offence and records will be studied to identify instances of such offenses. The NHS Counter Fraud & Security Management Service may also be contacted to investigate whenever fraud is suspected. I also understand that I will be charged the full cost should I mistreat or not take due care of the equipment issued.

2.3.7 With the exception of devices allocated to Resilience managers, all Trust mobiles are barred from making premium and international calls. If a user requires an international facility for an arranged period of time (max 30 days) then a request must be made via the ICT Service Desk. This request will be sent electronically to be authorised by the users Associate Director/Head of Service or Sector Commander. In the event the request is for an Associate Director the authorisation must be obtained from a Director.

2.3.8 Employees leaving the Trust must return their mobile device to the ICT service desk where possible; alternatively equipment can be returned to their own manager who must return equipment to ICT. The equipment should be in good condition (fair wear and tear acceptable) and have any supplementary devices with it i.e. chargers, cases, ear pieces.

2.3.9 All personal accounts should be removed from mobile phones prior to returning to the ICT Service desk so the device can be reused.

2.3.10 Mobile devices must not be passed from the nominated individual to other employees for temporary change in duties or be passed to another employee where the nominated user has left the Trust. If this happens the device and SIM will be suspended without prior notification until returned to ICT service desk and the correct request procedure followed.

2.3.11 Failure to return equipment or the return of damaged equipment may result in the employee being charged for a replacement.

2.3.12 Employees are responsible for all content of the device such as text and media that is stored, accessed or sent on Trust mobile devices. All information must be treated in line with the Data Protection Act and Information Governance guidelines. Disciplinary action may be taken against any member of staff found to have inappropriate material on a Trust device

2.4 Information Governance

2.4.1 Information Governance is the way by which the NHS handles all organisational information - in particular the personal and sensitive information of patients and employees. It allows organisations and individuals to ensure that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

2.4.2 It provides a framework to bringing together the requirements, standards and best practice that apply to the handling of information. It has four fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information;
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources;
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards;
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.

2.4.3 The framework currently encompasses:

- Data Protection Act 2018
- UK General Data Protection Regulation 2016 https://www.legislation.gov.uk/ukpga/2018/12/contents/enactedFreedom
- Freedom of Information Act 2000 -
- Confidentiality: NHS Code of Practice
- Records Management Code of Practice
-

2.4.4 The Yorkshire Ambulance Service NHS Trust (YAS) has a comprehensive Information Governance work plan managed by the Trust's Information Governance Working Group and coordinated by the Information Governance Team. Compliance is assessed by means of the annual Data Security and Protection Toolkit (DSPT) return.

3.0 Monitoring compliance with this Policy

3.1 The ICT department will monitor device usage and mobile phone bills regularly on a quarterly or ad hoc basis where required or requested. The ICT department will bring to the attention of the users line manager any suspected misuse of Trust issued devices.

3.2 The Trust also reserves the right to suspend SIMs and devices that have remained unused for a period of time no less than 6 months. Any telephone numbers may be re issued where required and are irretrievable. The individual will also be requested to return their equipment. Failure to do so may result in a charge for the full cost of replacement equipment to be levied from the responsible user.

4.0 Appendices

4.1 Appendix 1- Mobile Phone Acceptance Form

Mobile Phone Acceptance Form

Name:	Click or tap here to enter text.		
ESR No.	Click or tap here to enter text.	**Date:**	Click or tap to enter a date.
Work Address:	Click or tap here to enter text.	**Department:**	Click or tap here to enter text.
Mobile Number:	Click or tap here to enter text.		

Declaration

I agree to the disclosure of mobile device billing information for monitoring and evaluation purposes. In the event of excessive use for personal calls mobile data, inappropriate usage or fraudulent applications I am aware it is a disciplinary offence and records will be studied to identify instances of such offenses. The NHS Counter Fraud & Security Management Service may also be contacted to investigate whenever fraud is suspected. I also understand that I will be charged the full cost should I mistreat or not take due care of the equipment issued.

Name: Click or tap here to enter text.

Date**:** Click or tap to enter a date.

Signed: ________________________________

Please sign and return to: ICT service desk, Unit M