NHS
Yorkshire
Ambulance Service
NHS Trust

Mobile Device Allocation and Usage Policy

Document Author: Infrastructure & Voice Communication Manager

Date Approved: April 2026

Document Reference	ICT - Mobile Device Allocation and Usage – April 2029
Version	V: 5.0
Responsible Director (title)	Chief Information Officer (CIO)
Document Author (title)	Infrastructure & Voice Communication Manager
Approved By	Information Governance Working Group
Date Approved	April 2026
Review Date	April 2029
Equality Impact Assessed (EIA)	Yes
Document Publication	Internal only – Trust intranet

Document Control Information

Version	Date	Author	Status (A/D)	Description of Change
1.0	09/08/2017	Michael C Foster	A	Approved by TMG
2.0	Oct 18	ICT	A	Approved at TMG
3.0	Feb 2021	Risk Team	A	Approved at TMG
4.0	June 2023	Risk Team	A	Approved at TMG
4.1	December 2024	Risk Team	A	Formatted to Trust template.
4.2	July 2025	ICT	D	Review
4.3	December 2025	ICT	D	Additional updates and rewrite for iPads and all mobile device types
4.4	January 2026	Risk Team	D	Formatted to Trust template.
5.0	April 2026	Risk Team	A	Policy approved within April 2026 IGWG.
A = Approved D = Draft				
Document Author = Infrastructure & Voice Communication Manager				

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
Training and support available for all staff
Reasonable adjustments and accessible device options available

1.0 Introduction

1.1 This policy applies to all Yorkshire Ambulance Service NHS Trust (YAS) staff, contractors, and other NHS staff issued with or accessing Trust mobile devices.

1.2 It defines responsibilities for supply, usage, care, and governance of mobile devices, including smartphones, standard phones, tablets, and laptops.

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 Purpose/Scope

2.1 Resource Efficiency: Device allocation and refresh cycles will be managed to optimise resources, reduce costs, and support sustainability.

2.2 Role-Based Allocation: Devices are allocated based on role necessity, with Executive/Director, on-call, and mobile staff prioritised. Frontline 999 operational staff will transition to SIM-enabled iPads. In most cases home based workers will be expected to use Microsoft Teams. For any urgent situations or minor, time-sensitive needs where Teams access is not practical, staff may use their personal phones to make or receive calls. However, this should be limited to emergency or small-scale use only, and workers must continue to follow confidentiality and information governance guidelines when doing so.

2.3 Dormant Device Management: Devices unused for six months will be switched off and recalled. Monthly reviews will identify dormant devices for deactivation.

2.4 Device Type Review: Where appropriate, basic call/text devices may replace smartphones, reducing refresh frequency and costs. BYOD options will be explored.

2.5 Sustainability: Device disposal will prioritize recycling and potential resale, supporting Trust sustainability goals.

3.0 Process

3.1 Requisitions

3.1.1 Device entitlement is based on role criteria and must be authorised by an appropriate budget holder. All requests must go through the ICT Service Desk.

- Mobile Manager/ On call staff – Smartphone and/or laptop/tablet

- Frontline mobile staff (Ops, EOC, PTS, IUC) – Smartphone/Standard phone, tablet/laptop
- 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
- Home based staff – Laptop and MS Teams with personal mobile
- Staff who do not need access to restricted Trust applications may use their personal mobile devices for common Microsoft services such as email, Teams, and other applications, as well as for occasional calls. Where business specific requirements exist, a Trust-issued SIM or eSIM can be provided.

3.2 Trust Responsibilities

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

3.2.2 The Trust will

- Decide on device make/model for cost and management efficiency.
- Monitor device usage and suitability.
- Provide itemised bills on request.
- Ensure mandatory security measures (passwords, device encryption).
- Ensure compliance with Data Security Protection Toolkit (DSPT) and cyber risk assessments.

3.3 Training and Support

3.3.1 To ensure all staff can use Trust-issued mobile devices safely, effectively, and confidently, the Trust will provide appropriate support and training. This includes:

- **Clear and accessible training** on mobile device use, Information Governance requirements, and data security. Training will be available in a range of formats, including optional in-person refresher sessions for staff who may benefit from additional support.
- **Plain-language guidance**, written to be easy to understand and free from unnecessary technical terminology. Where appropriate, the Trust will also provide **easy-read, visual, or step-by-step materials** to support staff with different learning preferences or digital confidence levels.
- Ensuring line managers are aware of their responsibility to signpost staff to training resources and highlight any additional support needs early, reflecting the Trust's values of Kindness, Respect, Teamwork, and Improvement.

3.3.2 The Trust is committed to ensuring that all staff can clearly understand and follow the requirements of this policy, regardless of their background, language needs or digital confidence. To support this:

- Translated or language-adapted guidance will be made available where needed to ensure staff can fully understand mobile device responsibilities, reporting processes, and Information Governance requirements.
- Line managers must check understanding and provide additional explanation or support where required, ensuring that all staff can confidently use Trust-issued devices and comply with policy expectations.

3.4 Reasonable Adjustments and Accessible Device Options

3.4.1 To ensure that all staff can use Trust-issued mobile devices safely and effectively, the Trust will provide appropriate reasonable adjustments in line with the Equality Act. This includes:

- Accessible device options, such as devices with larger screens, text-to-speech or speech-to-text capability, simplified interfaces, or easy-grip protective cases where required.
- Provision of adaptive or assistive software where this supports staff with visual, physical, cognitive, or neurodivergent needs.
- Guidance for managers to help them identify, request, and implement reasonable adjustments based on individual staff needs.
- Ensuring that processes for reporting loss, damage, faults, or security concerns are accessible in multiple formats (phone, online forms, or supported verbal reporting through ICT or line management).
- Staff who are pregnant may request alternative or lighter mobile device options or adjusted carrying solutions if standard equipment is uncomfortable or impractical.
- Where appropriate, the Trust will offer lightweight or ergonomic device options or alternative equipment for staff who experience discomfort with standard devices.
- Suitable carry cases, belt clips, or protective equipment will be provided where required to reduce physical strain and support safe handling.
- Staff will be supported with guidance and training on safe charging, electrical safety checks, and general device care to reduce the risk of overheating, damage, or electrical incidents.

  Line managers should consider workplace adjustments (e.g., alternative devices, accessories, or carrying solutions) where needed due to physical comfort, mobility, or existing health conditions.

3.5 Mobile User Responsibilities

3.5.1 Mobile users are responsible for the day-to-day care of their device and must take all reasonable precautions to prevent damage, loss, or theft. Any incident involving damage, loss, or theft must be reported immediately via the **Datix incident management system** or by calling the Datix hotline at **0330 678 4070**, and then to the **ICT Service Desk** through the online portal or by telephone at **0330 678 4050**. Loss or theft should be reported as soon as identified to enable ICT to wipe or secure any data stored on the device. In cases of theft, the incident must also be reported to the police, and a crime reference number obtained.

3.5.2 At the discretion of the Trust, a charge for the full cost of replacement equipment and any unauthorised calls or usage may be levied from the employee, for example in cases of wilful misuse or failure to take reasonable steps to safeguard the device. The Trust expects all staff to take appropriate care of mobile devices; there is no insurance provision for phones, tablets or laptops. Any decision to apply replacement costs will consider the individual circumstances of the incident, ensuring fairness and proportionality. Staff may raise concerns about the application of charges through their line management or existing Trust support routes.

3.5.3 All mobile users should be aware that the mobile device that they have been provided with is for use on Trust business. Limited personal use which includes local, national and mobile calls as well as SMS text messages, where these are provided as part of an inclusive package is permitted.

3.5.4 Calls to premium-rate numbers and SMS text messages that incur additional charges are strictly prohibited unless prior authorisation has been obtained from ICT.

3.5.5 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.

3.5.6 Tethering, also known as using a mobile hotspot, is permitted only for authorised users. It should not be used on a regular basis and must be reserved for emergencies. Tethering is not a substitute for your home broadband. Many organisations provide access to guest or public wireless networks, most health organisations also support **govroam**, which is available to NHS Trust staff. Govroam can be used on both Trust and personal devices, and staff can log in using their personal YAS credentials.

3.5.7 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.

3.5.8 The Trust recognises the importance of maintaining healthy work life boundaries for staff with mobile or on-call duties. Expectations around availability must be clearly communicated by line managers and should relate only to defined periods of duty or agreed on-call arrangements. Staff will not be expected to routinely respond outside these times, and mobile devices should not create an implied obligation to be contactable when off-duty.

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

3.5.10 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 budget holder.

3.5.11 Mobile devices are not enabled for international roaming; therefore, mobile data will not work unless authorised for business purposes by the relevant budget holder. Wi-fi connectivity will continue to work if connected to a suitable, secure Wi-Fi network. Please note that roaming from certain countries is prohibited due to security concerns. For further details, please liaise with the Service Desk.

3.5.12 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).

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

3.5.14 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.

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

3.5.16 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.

3.6 Bring Your Own Device (BYOD)

3.6.1 Purpose/Scope

3.6.1.1 The Trust recognises that some staff may prefer to use their personally owned mobile devices for work purposes. BYOD supports flexibility, cost control and operational efficiency where it is safe and appropriate to do so. This section applies to any personal phone, tablet or laptop used to access Trust information or services.

3.6.2 Eligibility

3.6.2.1 BYOD is available to staff whose roles do not require a Trust-issued device and where operational needs can be safely met. The Trust may require a Trust-issued device in cases of operational necessity (for example, rurality, lack of alternative access, or specific business needs).

3.6.3 Acceptance and Conditions of Use

3.6.3.1 Staff must accept the Trust's BYOD Acceptable Use Statement (see Appendix) before using a personal device for Trust business. BYOD use must comply with all relevant Trust policies and national guidance.

3.6.4 Mandatory Security Controls

3.6.4.1 Personal devices used for BYOD must meet the following minimum standards:

- A strong passcode or biometric lock must be enabled, and full device encryption must be active.
- The operating system must be supported by the vendor and kept up to date with security patches.
- Staff must use approved, secure applications (for example, Microsoft 365 and Microsoft Teams) for Trust communication and data. Consumer messaging applications must not be used for Trust information unless explicitly authorised by the Trust.

3.6.5 Access to NHSmail and Microsoft 365

3.6.5.1 Access from BYOD to NHSmail or Microsoft 365 is subject to Conditional Access policies and Multi-Factor Authentication (MFA). Access from unmanaged devices may be restricted in line with NHSmail BYOD security controls.

3.6.6 Information Governance Requirements

- Staff must not store patient or confidential Trust information on a personal device unless strictly necessary and only with approved safeguards (for example, secure app containerisation).

- Personal device backups must not cause Trust data to be stored outside the UK/EEA or in unapproved cloud services.
- Staff must provide any Trust-related information held on a personal device if required to meet Freedom of Information (FOI) or GDPR/Subject Access Request (SAR) obligations.
- Use must comply with the Trust's Data Protection, Records Management and Information Governance policies, and applicable national standards (including the Data Security and Protection Toolkit and, where relevant, DLP/sensitivity labels).

3.6.7 Privacy, Monitoring and Revocation

3.6.7.1 BYOD devices may be subject to technical checks needed to protect Trust data (for example, Conditional Access and MFA). The Trust does not collect personal content from BYOD; any monitoring is undertaken solely for cost control, contract management and security, and not to assess individual performance. The Trust may revoke BYOD privileges where compliance or security standards are not met.

3.6.8 Incident Reporting

3.6.8.1 Loss, theft, suspected compromise, or misdirected data involving a personal device used for Trust business must be reported immediately through Datix and to the ICT Service Desk so appropriate actions can be taken (for example, selective wipe of corporate app data or containers).

3.6.9 Responsibilities, Costs and Support

3.6.9.1 Staff are responsible for the care, security and appropriate use of their personal device. The Trust will cover the cost of the YAS SIM/eSIM and associated business usage. The Trust will not reimburse the purchase, maintenance or repair of personal devices. Technical support for BYOD is limited to SIM/eSIM and Trust applications. Staff may opt out of BYOD and request a Trust-issued device if their role or circumstances change, subject to approval and resource availability.

3.6.10 Local assurance

3.6.10.1 The Trust will maintain a Data Protection Impact Assessment (DPIA) for BYOD and align controls with relevant national security guidance, including NHS England BYOD guidance, NHSmail BYOD security controls and NCSC BYOD good practice.

3.7 Information Governance

3.7.1 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.

3.7.2 It provides a framework to bring 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.

3.7.3 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

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

3.8 Privacy and Information Governance Requirements

3.8.1 The Trust is committed to ensuring that all staff can use mobile devices safely, securely, and with confidence that their personal information — and the information of colleagues and patients is always protected. To support this, the following measures apply to all Trust issued mobile devices:

- **Reinforced Information Governance controls**, ensuring all staff follow Trust policies on the secure handling, storage, and transmission of personal and sensitive data.
- **Clear guidance for staff** on protecting confidential information when using mobile devices, including:
    - Using approved Trust applications for communication and data access.
    - Avoiding the storage of unnecessary personal or sensitive information on devices.
    - Ensuring screens are locked when devices are unattended.
    - Reporting any suspected data breaches or privacy concerns immediately via the appropriate channels.
- Mobile devices must be used in a way that upholds **privacy, dignity and confidentiality** for patients, colleagues, and members of the public.
- Staff must not access, share, or disclose personal or confidential information unless they have a lawful and legitimate reason to do so.
- All staff must complete mandatory Information Governance training and follow any additional guidance issued by ICT or the Information Governance Team regarding safe device use.

4.0 Implementation Plan

4.1 The latest approved version of this document will be posted on the Trust Intranet site for all members of staff to view. New members of staff will be signposted to how to find and access this guidance during Trust Induction.

5.0 Monitoring compliance with this Policy

5.1 The ICT department will monitor device usage and mobile phone bills regularly on a monthly or ad hoc basis where required or requested. This monitoring is carried out solely for cost control, contract management, and security purposes, and is not used to

assess individual performance or day-to-day activity. The ICT department will bring to the attention of the user's line manager any suspected misuse of Trust-issued devices.

5.2 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.

6.0 Appendices

6.1 This Policy includes the following appendices:

Appendix A - Bring Your Own Device (BYOD) Acceptable Use Statement

Appendix A – Bring Your Own Device (BYOD) Acceptable Use Statement

Purpose:
This Acceptable Use Statement sets out the responsibilities and required security standards for any member of staff using a *personally owned device* to access Yorkshire Ambulance Service NHS Trust (YAS) systems or data.
It must be read, understood and accepted before BYOD access is granted.

---

1. Security Requirements
By using my personal device for Trust business, I agree to:

1. Use a **strong passcode, PIN or biometric lock** on the device.
2. Ensure the device has **full-device encryption** enabled.
3. Keep the device's **operating system updated** with all current security patches.
4. Use only **approved, secure Trust applications** (e.g., Microsoft 365, Microsoft Teams) for any work-related communication or data access.
5. Accept and comply with **NHSmail BYOD Conditional Access policies** and **Multi-Factor Authentication (MFA)** where required
6. Ensure the device is free from malware, unauthorised configuration changes, or software that may compromise security.

---

2. Information Governance & Data Protection
I understand and agree that:

1. I must **not store patient or confidential staff information** on my personal device unless strictly necessary and only when approved secure apps or containerisation are in use.
2. Trust data must **not be backed up** to personal cloud services, external accounts, or any location outside the UK/EEA that is not approved by YAS.
3. I must never use consumer messaging apps (e.g., WhatsApp, Facebook Messenger, SMS) for Trust information unless explicitly authorised under an approved SOP.
4. Screens must be protected from unauthorised viewing; the device must auto-lock when not in use.
5. If required, I must provide any Trust-related information stored on my device to assist with **Freedom of Information requests (FOI)** or **Data Subject Access Requests (SAR)**.

---

3. Incident Reporting & Cooperation
I agree to:

1. **Immediately report** any loss, theft, suspected compromise or unauthorised access involving my personal device to Datix and the ICT Service Desk.
2. Cooperate with the Trust in protecting YAS data on my device, including permitting a **remote selective wipe** of Trust applications or data if required for security.
3. Not attempt to circumvent Trust security controls, policies or monitoring mechanisms.

---

4. Appropriate Use
I understand that:

1. My personal device remains my responsibility, including repair, replacement and maintenance.
2. The Trust will fund the cost of any **YAS SIM/eSIM and associated business usage**, but not the device itself.

3. The Trust may **revoke BYOD access** if I fail to meet security, compliance or usage requirements.
4. I must only use my personal device for Trust purposes where this is appropriate to my role and authorised by my line manager.
5. I must comply with all relevant Trust policies, including Information Governance, Cyber Security, Records Management, Confidentiality and Data Protection.

---

5. Acceptance

By signing below, I confirm that:

- I have read, understood and agree to comply with this BYOD Acceptable Use Statement.
- I understand that failure to comply may result in removal of BYOD access, disciplinary action, and/or security investigation.
- I understand that this statement complements, but does not replace, existing YAS Information Governance and security obligations.

Name	
Role/Department	
Date	
Signature	