East of England
Ambulance Service
NHS Trust

Policy for
Control of Mobile Devices

Document Reference:	POL063
Document Status:	Approved
Version:	V4.0

DOCUMENT CHANGE HISTORY

Initiated by	**Date**	**Author (s)**
Head of IM&T	January 2011	IM&T Security & Resilience Manager
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
2.0	March 2013	Reviewed by IT Security & Resilience Manager
2.1	February 2013	Reviewed by IT Security & Resilience Manager
3.0	April 2019	Reviewed by IT Security & Resilience Manager

Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
3.1	April 2019	Reviewed by IT Security & Resilience Manager
3.2	May 2019	Approved at IGG
4.0	June 2019	Approved by MAG
5.0	August 2021	Approved by CRG

Document Reference	POL063 Directorate: IM&T
Recommended at **Date**	Information Governance Group 15 July 2021
Approved at **Date**	CRG 16 August 2021
Valid Until Date	August 2023
Equality Analysis	June 2021
Linked procedural documents	None
Dissemination requirements	All staff
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Appendices

1. Introduction

In certain circumstances having use of a portable mobile device can assist the staff in carrying out their duties therefore the Trust has made a significant investment in mobile devices.

2. Purpose

This policy defines the approach to be taken in the management of these devices to ensure appropriate standards are met, value for money is maximised and appropriate disposal measures are undertaken.

The objectives of the policy are to ensure Trust staff are aware of their responsibilities with regards to these devices and to ensure the reliability, resilience, maintainability, and supportability of these devices.

3. Duties

3.1 All Staff

Are responsible for using the equipment in a safe and controlled manner at all times.

Are responsible for identifying faulty equipment and informing the IM&T Department via the IT Service Desk so a resolution can be found.

Are responsible for identifying redundant equipment, informing the IM&T Department, and following IM&T processes for the correct disposal of equipment.

Are responsible for using the equipment in accordance with this policy

Are responsible for the safe storage and use of the equipment when not in use.

3.2 Line Managers

Are responsible for identifying which of their team members require mobile devices.

Are responsible for ensuring all requests for devices go through the IT Service desk.

Are responsible for notifying the IM&T Department of any change in business requirements that will necessitate a change in provided equipment, whether that be returning the device to the IM&T department or reallocation to another team member.

Are responsible for ensuring any DSE assessments are reviewed for staff receiving equipment.

3.3 Head of Live Services

Is responsible for implementing an equipment replacement programme as and when applicable.

3.4 IM&T Operational Staff

Are responsible for identifying equipment requiring replacement and managing the process of replacement and disposal in their areas.

3.5 Head of Live Services\IM&T Management Team

Are responsible for preparing any required business cases for obtaining capital or revenue funding required for large scale replacement of systems related to these devices.

4. Consultation and Communications with Stakeholders

Consultation will be via the departmental and staff representatives on the Information Governance Group, and when agreed will be communicated to all staff.

5. Definitions

Mobile Device: Any device capable of data or voice communications. For the purposes of this policy this does not include Airwave radio equipment.

6. Development

6.1 Prioritisation of Work

Devices will be provided by the Trust to staff meeting the following criteria:

a) Staff are out of the office on business on a regular basis (half the week or more) or by the nature of their role must be contactable

or

b) Staff who have on call duties or who are required in the event of an emergency;

or

c) Staff who fulfil certain roles and need to be contactable (e.g. signatories for certain key processes)

Ultimately, senior managers are responsible for determining who requires a device in accordance with Trust business needs, and IM&T staff will determine the most appropriate device.

6.2 Identification of Stakeholders

Stakeholders will be all staff requiring a mobile device, their line management and IM&T.

6.3 Responsibility for Document's Development

The development of this document is the responsibility of the IM&T Security and Resilience Manager, in conjunction with other senior IM&T managers.

7. Requesting a Mobile Device

All requests for mobile devices must be submitted to the IT Service Desk, either via email or via the self-service portal.

7.1 Issuing of Devices

To ensure the best use of limited resources a single device will be issued to staff, either a device capable of voice only, or one capable of voice and data communications. Exceptions will only be permitted where it is deemed by senior management that a degree of resilience is necessary.

7.2 Personal Use

Staff should only use Trust issued mobile phones for personal calls in urgent or emergency situations, as mobile phones are provided for business use. As an exception where a member of staff is on call a short personal call at local rates of up to five minutes is considered acceptable. The Trust's finance department may consider the recovery of costs associated with private use if they arise.

7.3 Non-Trust Owned Devices

Data can only be stored on encrypted equipment owned and supplied by the Trust. Attempting to setup access on any device that results in data being stored on that device, may result in disciplinary action.

An exception is in place for personal mobile phones and tablets whereby they are permitted to connect to the Trust email system. The configuration details for this must be requested via the IT Service Desk standard procedure.

The device must be encrypted to conform to Trust and National policy. Encryption is activated automatically with Smartphones (iPhones, Android, Nokia, etc.) and a passcode enforced when connected to an Exchange server.

Staff must be aware that by configuring personal devices to receive Trust email they are automatically allowing IT to control their device. This is purely for security purposes; IM&T cannot access personal devices or the information on it. However, IM&T will have the ability to remotely wipe personal devices completely should they be lost or stolen. The device will be reset to factory settings if this is necessary. Staff have a duty to inform IM&T as soon as possible should your device be lost or stolen. If staff are not happy for IM&T to have this ability, then they should not configure personal devices to receive Trust email. Staff will still have the ability to connect to Trust email using the web browser on your personal devices without any configuration required and without giving IT the ability to remotely wipe the device.

Staff should note that although using personal devices to connect to Eastamb email is permitted; the device, it's connectivity and configuration are not supported by IM&T. Should staff need assistance with setting personal devices up they should seek assistance from their mobile providers.

Connection to the Trust email is permitted via the Internet from all connected devices via Microsoft Office 365, the connection details for this must be requested via the IT Service Desk standard procedure. When using this facility staff must not allow browsers to store any logon details.

7.4 Using Mobile Devices Whilst Driving

Staff should adhere to current legislation regarding the use of use mobile devices whilst driving a vehicle. If it is deemed necessary by senior management that an individual may be required to use a mobile phone whilst driving then arrangements must be made via the Fleet department to have a suitable hands-free kit fitted to the vehicle(s).

7.5 Confidentiality

Staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information. A breach of confidential information whether patient related, commercially confidential, in respect of staff and colleagues or any other sensitive information is a serious incident and will be subject to management action under the Trust's disciplinary policy.

7.6 Use of Mobile Devices on Other Sites

Many organisations, particularly in the NHS, have local rules regarding the use of mobile devices and these must always be respected.

7.7 Disposal of Mobile Devices

Staff should not dispose of any device themselves, they must return them to their local IT Department who will arrange disposal.

7.8 Register of Mobile Devices

A record of all mobile devices will be kept by IM&T. This record will detail the mobile device number, and name of person to whom the mobile device is issued. No mobile device may be transferred to another member of staff without authority from, and in arrangement with, IM&T.

Staff will be responsible for producing the device that is allocated to them if requested by IM&T staff or their manager.

7.9 Loss, Theft or Damage of a Mobile Device

All losses, thefts or damage to a mobile device should be reported to IM&T as soon as is practicable.

8. Equality Impact Assessment

This is attached, Executive Summary is in Appendix B

9. Dissemination and Implementation

9.1 Dissemination

This policy will be held in the document library and advertised in line with the Trust policy on dissemination of procedural documents.

It will be circulated within IM&T via the senior management team

9.2 Implementation

Technical implementation is currently in place in line with this policy, current legislation and best practice. IM&T staff will be expected to be experienced in these areas, any training needs will be identified via the PDR process and arranged.

10. Process for Monitoring Compliance and Effectiveness

As per 7.2 audits will be undertaken on compliance with the policy to ensure that mobile devices are being used for business purposes only.

10.1 Breaches of Policy

Failure to comply with the above procedure or misuse of any mobile device may result in Disciplinary action.

11. Standards/Key Performance Indicators

A service call will be scheduled monthly to carry out audits as per 7.2. See also Appendix B.

12. Associated Documents

Information Security Policy

IM&T Operational Security Policy

Appendices

A	Monitoring Table
B	Equality Analysis

Appendix A

Monitoring Table

What	Who	How	Frequency	Evidence	Reporting arrangements	Acting on recommendations	Change in practice and lessons to be shared
Functionality and adherence to policy	IT technical staff	Use of monitoring systems, MDM, Azure, PRTG, etc	Continual monitoring will take place as part of the day to day function of IM&T.	Evidence will be provided information logged in the Service Desk call management system, the asset management system and manufactures warrantee information	Reporting will be via line management	The IM&T management team will undertake subsequent recommendations and action planning for any or all deficiencies and recommendations within reasonable timeframes.	All changes will be documented on the call logging system and a report sent to the appropriate Service Delivery Manager

Appendix B – Equality Impact Assessment

EIA Cover Sheet	
Name of process/policy	IM&T Mobile Device Policy
Is the process new or existing? If existing, state policy reference number	POL063
Person responsible for process/policy	IT Security & Resilience Manager
Directorate and department/section	Strategy & Sustainability
Name of assessment lead or EIA assessment team members	IT Security & Resilience Manager
Has consultation taken place? Was consultation internal or external? (please state below):	Via email
Internal	Head of IM&T
	Deputy Head of IM&T
	IT Infrastructure Service Delivery Manager
	IT Service Desk Service Delivery Manager

The assessment is being made on: Please tick whether the area being assessed is new or existing.	Guidelines	
	Written policy involving staff and patients	X
	Strategy	
	Changes in practice	
	Department changes	
	Project plan	
	Action plan	
	Other (please state) Training programme.	

Equality Analysis

What is the aim of the policy/procedure/practice/event?

To provide instruction and guidance with regards to the use of mobile devices.

Who does the policy/procedure/practice/event impact on? Nobody

Race	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Who is responsible for monitoring the policy/procedure/practice/event?

IT Security & Resilience Manager

What information is currently available on the impact of this policy/procedure/practice/event?

None

Do you need more guidance before you can make an assessment about this policy/procedure/ practice/event?

No

Do you have any examples that show that this policy/procedure/practice/event is having a positive impact on any of the following protected characteristics? Yes/No, If yes please provide evidence/examples:

Race	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Please provide evidence:

No

Are there any concerns that this policy/procedure/practice/event could have a negative impact on any of the following characteristics? Yes/No, if so please provide evidence/examples:

Race	□	**Religion/belief**	□	**Marriage/Civil Partnership**	□
Gender	□	**Disability**	□	**Sexual orientation**	□
Age	□	**Gender re-assignment**	□	**Pregnancy/maternity**	□

Please provide evidence:

No

Action Plan/Plans - SMART

Specific

Measurable

Achievable

Relevant

Time Limited

None required

Evaluation Monitoring Plan/how will this be monitored?

There is zero impact on any "characteristic" therefore there is no need to monitor.