NHS
East Midlands
Ambulance Service
NHS Trust

# Portable Device Usage Policy

**Links**

The following documents are closely associated with this policy/procedure/SOP:

- Information Security Management: NHS Code of Practice (Apr 2007)
- IM&T Security Policy
- Untoward Incident Reporting Policy
- IM&T Bring Your Own Device (BYOD) Policy

| | |
|---|---|
| **Document Owner :** | Director of Strategy and Information |
| **Document Lead:** | Head of IM&T |
| **Document Type:** | IM&T Policy |
| **For use by:** | All Trust employees utilising portable devices |

| | |
|---|---|
| Equality Impact Assessment | *N/A* |

| **This document has been published on the:** | |
|---|---|
| **Name** | **Date** |
| Library (EMAS Public Drive) | 28 March 2017 |
| Intranet | 28 March 2017 |

| **Version Control** | **Document Location**<br>If using a printed version of this document ensure it is the latest published version.<br>The latest version can be found on the Trust's Intranet site. |
|---|---|

| Version | Date Approved | Publication Date | Approved By | Summary of Changes |
|---|---|---|---|---|
| 1.0 | 25 April 2013 | *April 2013* | ICT Security Group | New Policy |
| 2.0 | 27 March 2015 | 16 November 2015 | Information Governance Group | Annual review.  Updated section 19.5 to clarify driver expectations in line with the Road Traffic Act 1988. |
| 3.0 | 28 January 2016 | 10 February 2016 | Information Governance Group | Review to amend provisions and details regarding use of mobile telephones. |
| 4.0 | 23 March 2017 | 28 March 2017 | Information Governance Group | Annual review. Updated policy to remove BlackBerry devices and replace with smartphones. Removed all references to the Fraud and Corruption Policy which expired in 2010. |
| | | | | |
| | | | | |

**Contents** **Page**

## 1. Introduction

1.1. This document references the IM&T Security Policy and is only to be used in conjunction with said Policy.

1.2. All EMAS personnel using Portable Devices are to comply with the IM&T Security Policy which is based upon elements of ISO27001. Unauthorised modification and/or amendment of this document are forbidden.

1.3. The purpose of this policy is to ensure that staff (and visitors they have invited on to EMAS premises) using portable devices are aware of the security risks associated with these and the controls they need to follow to minimise loss of data and/or device.

## 2. Objectives

2.1. The objective of this policy is to protect the security and integrity of EMAS' data and portable devices.

## 3. Scope

3.1. This document applies to all employees of the Trust including permanent, temporary, voluntary and contract staff utilizing EMAS owned portable devices; including their own used for corporate purposes under the Bring Your Own Device (BYOD) policy.

## 4. Definitions

4.1. **Anti-Virus Software –** software installed on devices to protect from infection

4.2. **BYOD** – Bring Your Own Device; a policy that allows staff to use a personal device for corporate purposes, subject to specific controls being applied by EMAS' IM&T Department

4.3. **Call Reference Number** - Number generated when a ticket is raised by the IM&T Service Desk

4.4. **Encryption Software –** software installed on devices to protect sensitive data

4.5. **HSCN –** Health and Social Care Network (transition from N3 commences 2017)

4.6. **IM&T Portal –** Service Management tool used by the IM&T Department for handling incidents, requests and changes

4.7. **Information Commissioner's Office (ICO)** - Office responsible for the enforcement of the Data Protection Act 1998, and also responsible for Freedom of Information

4.8. **MDM** – Mobile Device Management; applications applied to a mobile device that allow (for example, but not limited to) EMAS IM&T staff to remotely manage, or delete applications and data on that device

4.9. **N3** – NHS spine network provided by BT

4.10. **Personal Identifiable Information (PII)** - information that can be used to identify an individual

4.11. **Portable Devices** - are defined as Laptop, Tablet and Notebook computers, Cameras and mobile telephones, including CD/DVDs and paper records

4.12. **PSN –** Public Service Network

## 5. Responsibilities

5.1. **IM&T Department** - IM&T staff will act as the delegated agents of the Chief Executive and are responsible for maintaining a safe and secure computing environment in EMAS. IM&T will provide by request portable devices and ensure the user reads this policy and signs the Portable Device Acceptance form, demonstrating understanding. The signed appendices will be scanned and stored in a secure location for reference.

5.2. **EMAS Line Managers** - EMAS Line Managers shall ensure that staff comply with this policy and understand the implications of non-compliance. IM&T will work with EMAS Line Managers to ensure all portable devices are recovered when a user leaves EMAS or moves to a role where a device is no longer required.

5.3. **EMAS Employees** - EMAS Employees will comply with this policy and understand the implications of non-compliance.

## 6. Hardware Control

6.1. The responsibility of ultimate control for issue and security of Portable Devices lies with the Trust Chief Executive. Delegated responsibility has been assigned to the Head of IM&T.

## 7. Information Security

7.1. Only authorised staff are allowed access to and use of the allocated Portable Devices. Persons accessing data on N3, HSCN (or PSN) and using it for health related purposes, should afford all material stored and processed on these systems adequate protection.

## 8. Physical / Hardware Security

8.1. The following guidelines should always be adhered to by the user of the Portable Device:

- *Treat the Portable Device as if it is your own property*
- *The Portable Device must be kept in secure accommodation when not in use*
- *Portable Device security is your responsibility at all times*
- *Wherever possible, all Portable Devices; shall be transported in the vehicle's locked boot*
- *If, due to the amount of hardware, media or paper records being transported, the requirement is to be carried in the interior of the*

*vehicle, they shall be covered with a cloth or blanket and secured in an appropriate manner*

- *If possible, the doors of the vehicle and the boot shall be locked even whilst the vehicle is in motion*
- ***Remove** Portable Devices, containing PII or confidential data from unattended vehicles*
- ***Do not** leave the Portable Device unattended anywhere that is unsecure*
- *The Laptop/Notebook must have a BIOS password enabled*
- *The Laptop/Notebook must be encrypted*
- *All Portable Devices must have a security asset tag affixed or be identifiable via an IMEI number in the case of a mobile telephone*
- *The Mobile Telephone must have a password enabled*
- ***Do not** leave your Smartcard in the same location as the Portable Device*
- ***Do not** keep password details in the same location as the Portable Device*
- *Avoid leaving the Portable Device within sight of ground floor windows or within easy access of external doors*
- *All removable media must be afforded the same level of security as the Portable Device*
- *Take care to avoid the risk of overlooking by unauthorised persons when using Portable Devices in public places*

## 9. Software Security

9.1. All laptop/notebooks must have encryption software installed. Users of Portable Devices are not authorised to load any software onto the Portable Device without first requesting permission to do so, via the IM&T Portal and receiving subsequent authorisation.

## 10. Virus Control

10.1. The Portable Device must have an Anti-Virus software package installed (excludes mobile phones). Users are not to alter the configuration of this package. The anti-virus system's database of virus definitions will be updated on a regular basis, each day if possible by the EMAS IM&T Department.

10.2. The Anti-virus software package has been installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

10.3. If a virus is discovered the following actions must be carried out:

- *Turn the Device off and disconnect from any network*
- *Place a label over the power switch, and CD/DVD drive stating that the machine has a virus infection and should not be used*
- *Isolate any CD/DVD disks that have been used on that machine*

- *Inform the IM&T Service Desk and immediate Line Manager*
- *The EMAS IM&T Department will have the software and technology available to eradicate any infections*
- *All virus infections will be assessed by the IM&T Security Group to decide whether they are significant enough a risk to be reported to the Department of Health and CareCERT*

## 11. Password Security

11.1. Password and Smartcard PIN Security are the responsibility of the individual. Passwords should be formulated in such a way that they are easily remembered but difficult to guess. It must conform to the EMAS password guidelines laid out in the IM&T Security Policy, and in most cases the guidelines laid out below are forced via the EMAS Group Policy.

- *Passwords and PINs must be kept confidential*
- *Paper records of passwords and PINs must* ***not*** *be kept*
- *Under no circumstances should a record of the password or PINs be kept with the device it relates to*
- ***Do not*** *share EMAS passwords or PINs with anyone, including administrative assistants or secretaries*
- *All passwords and PINs are to be treated as sensitive, confidential EMAS information*
- *Passwords must be changed regularly, at intervals not exceeding 31 days*
- *Three attempts to enter an invalid password will cause the user to be locked out*
- *Passwords must consist of a minimum of 8 characters*
- *Passwords must contain both upper and lower case characters and digits*
- *Passwords must* ***not*** *use consecutive characters (e.g. aaabbb, 123456)*
- *Passwords must* ***not*** *relate to the system or the user, although passwords should be easy to remember*
- *The password selected may not be the same as any of the previous six*
- ***Do not*** *use the same password for EMAS accounts as for other non-EMAS access (e.g. personal Internet Service Provider)*
- *Passwords and PINs must* ***not*** *be inserted into e-mail messages or other forms of electronic communication, although it is acceptable to send a password protected file via email, with a password sent via SMS to unlock the protected file*
- *Passwords and PINs must* ***not*** *be displayed on screens as they are entered*

- *All laptops and EMAS issued smartphone/android devices have an authorised protected 'screen lock out' enabled which will be displayed after 5 minutes of inactivity*

## 12. Internet / e-mail

12.1. The Portable Device has been provided by the organisation for use away from the users' approved base. It should be noted that the Internet is an uncontrolled, unmanaged and largely unsupported global network and has a large recreational attraction. It is a source of much valuable information, not least on the area of healthcare, however it is filtered and monitored by the EMAS IM&T Department.

12.2. Personal access to the Internet can be limited or denied dependent of the service needs. Staff must act in accordance with the Trust's guidelines. The Head of IM&T, assisted by the Information Governance Group, has the final decision on deciding what constitutes excessive or inappropriate use.

12.3. Access to the Internet is permitted primarily for healthcare and work related purposes and reasonable use is permitted provided that:

- *this does not interfere with the performance of your duties*
- *the activities do not impinge upon the performance of the network*
- *the activities do not infringe the conditions of the IM&T Security Policy*
- *No illicit or illegal material will be viewed/downloaded or obtained via the Internet or e-mail*
- *The user will make their system available at any time for audit either by the EMAS IM&T Department and/or representatives of the Department of Health*
- *Breaches of security, abuse of service or non-compliance with the N3 Code of Connection may result in the withdrawal of all N3 services including e-mail*
- *EMAS reserves the right to monitor e-mail and internet usage if there is a suspicion of breach of policy, attack vectors, suspicious browsing, misuse etc.*

## 13. Maintenance

13.1. Maintenance is to be controlled by the EMAS IM&T Department. If possible, all equipment that requires repair or maintenance that necessitates the equipment leaving EMAS premises must have patient sensitive/confidential information removed from it.

13.2. If the hard disk has failed and the maintenance engineer is required to replace it with a new device then the old hard disk must be retained by the EMAS IM&T Department for physical destruction. If the hardware is returned to the supplier for repair, a note of all serial numbers should be taken, including the hard disk. If the hard disk is irreparable, EMAS IM&T Department must insist that the old hard disk be returned for physical destruction.

## 14. Backup

14.1. It is the user's responsibility to ensure that their data and files are saved in a suitable location on the EMAS network, but should any files need to be stored locally to the Portable Device that regular backups are taken and stored on the EMAS network.

## 15. Losses and Confidentiality / Security Breaches

15.1. Incidents that constitute a loss of hardware or data, which could potentially lead to a breach of data confidentiality, are to be reported directly to the immediate line manager, IM&T Department and Head of Information Governance, via the IR1 process (Ulysses). The Trust Risk and Safety Team will instigate investigation procedures to try and establish the nature and potential threat of the incident. All such losses, as identified as being a Serious Untoward Incident, will be reported to the ICO via the Information Governance Toolkit Incident Reporting Tool as detailed in the Untoward Incident Reporting Policy.

15.2. Incidents could involve:

- *Loss of Hardware*
- *Loss of Software/Data*
- *Virus attack*
- *Unauthorised access*
- *Misuse of System and / or Privileges*
- *Loss of Personal Identifiable Information*
- *Loss of confidential information*

15.3. If a mobile phone is lost, the approved user of that device *may* be liable to the full present-day cost of a replacement, if an investigation proves to be that the user did not adhere to the requirements of this policy.

## 16. Accounting and Audit

16.1. The software and information held on Portable Devices is subject to the same audit procedures as the Trusts computer systems. This also covers information and data stored on removable media e.g. CD/DVDs.

## 17. Summary of Risks (non-exhaustive)

- *Mobile working requirements are increasing which could impact confidential and/or Personally Identifiable Information (PPI)*
- *Unsecure parking and high levels of crime in certain locations*
- *Different types of mobile data storage devices including laptops, PDA's, mobile telephones, USB memory sticks, portable hard disks, iPads, digital cameras etc….*
- *Amount of virus and spy ware threats and infections increasing in volume and complexity*

## 18. Use of USB Storage Devices

18.1. USB storage devices, such as those listed below, pose a very real threat to EMAS, the network and data that we hold on behalf of a large number of persons.

18.2. Therefore, any use of these USB storage devices is not permitted within EMAS and they are blocked from use (unless requested and approved via a request submission on the IM&T Portal). The EMAS IM&T Department actively scan the network and are automatically alerted when an unauthorised USB device is plugged in to a laptop. The devices include (but are not limited to):

- *USB Memory Sticks (permission required for use)*
- *USB External Zip Drives*
- *USB External Disk Drives*
- *Flash Memory Cards*
- *iPads*
- *MP3 Players*
- *Digital Cameras (permission required for use)*

18.3. When permission is granted for use of a USB device, the user must agree to the terms of use and follow the relevant guidelines.

18.4. Digital Cameras can be requested on an individual basis, through the submission and approval of a Request via the IM&T Portal.

18.5. When permission is granted for use of a digital camera, the user must follow and adhere to the following:-

- *Pictures should only be taken of individuals with the consent of that person*
- *The subject of the picture should be told what it will be used for and who it may be disclosed to*
- *The user must be conscious of the need to respect an individual's privacy*
- *The user must be aware of what or who else may be captured in the photo (not just the main subject) i.e. what/who is in the background*
- *Extra care must be taken with the security of the device if personal information is going to be stored on there*

## 19. Mobile Telephone Devices

19.1. The benefits for use of a mobile telephone device within a business setting are widely recognised.

19.2. This policy is designed to ensure both compatibility of the mobile phone device with existing PC/Laptop and Network Systems and also ensure the security and confidentiality of the data that these devices hold[1].

19.3. **Eligibility**

19.3.1. Mobile telephone devices will only be issued by the Trust to staff who fall within the following categories, and following receipt of a request made via the IMT Portal:

- Staff who are regularly required to travel in the course of their duties away from their contractual work base, **and** who have no alternative means of communications, or;
- Staff who are required to work alone, or;
- Staff who are required to participate in the Trusts' on-call system

19.3.2. All other requests for the provision of mobile telephone devices must be supported by appropriate justification from an Executive level Director of the Trust.

19.3.3. The Head of IM&T reserves the right to refuse any request which does not meet the above criteria.

19.4. **Device Choice**

19.4.1. All mobile telephone devices provided by EMAS will be selected by IM&T based on an evaluation of the device functionality, security and control functionality.

19.4.2. Only devices approved by the IM&T Department will be issued; requests for non-standard devices will not be approved.

19.4.3. Where a member of staff wishes to use their own mobile telephone device under the BYOD policy (refer separate policy document), then this will need to be requested via the IM&T request process. All such requests will be evaluated, and if subsequently approved will be subject to the end-user agreement policy that EMAS IM&T Department will install the MDM application on the device, and that the Trust have express permission to delete any data contained within the MDM environment at any time.

19.4.4. At the time of writing, only devices running Android Version 5.1 (Lollipop), Windows 8.1 or iOS 8.4 operating systems and above will be supported by the IM&T department under the BYOD policy. Other operating system based devices (eg Symbian – largely used in older Nokia devices) will not be supported.

19.5. **Security**

- *IM&T Department must ensure that mobile telephone devices are always configured to request a password on power-up and also when left idle*

[1] *PTS devices must remain on station when not in use*

- *Users shall ensure that whenever the mobile telephone device is left unattended, it must either be powered off or the password protect screensaver activated (in a similar way to that on your laptop/PC)*
- *IM&T Department must ensure that mobile telephone devices are encrypted*
- *Confidential information and/or Patient Identifiable Information (PII) shall not be downloaded to the mobile telephone device*
- *IM&T Department will apply controls and restrictions on the use of the mobile telephone device using a Trust approved MDM solution; all applications used for corporate purposes may be restricted to running within the MDM environment on the device*

### 19.6. Personal Calls

19.6.1. EMAS accept that devices may be used for personal calls, and are only to consist of standard rate landline and mobile numbers and should not include premium rate text services.

19.6.2. Random audits of individual mobile telephone call charges will be undertaken; any calls which are made to premium rate services will be charged to the end user, and deduction made from salary to cover those costs.

### 19.7. Premium Rate Phone Numbers / Premium Rate Text Services

19.7.1. These services are not to be accessed using an EMAS issued device. Any attempt to do so will be classed as misuse or abuse and reported directly to the department or divisional managers for action.

19.7.2. In cases of suspected fraud, including excessive and inappropriate use of the mobile phone, the matter will be referred to the Trust's nominated Local Counter Fraud Specialist for investigation.

19.7.3. The IM&T Department are able to disable these services via the network.

### 19.8. International Roaming

19.8.1. International Roaming is disabled on all devices by default. In exceptional circumstances a request which is authorised by a line manager will be approved if a business justification is provided. Activation will only be provided for a limited period.

### 19.9. Driving/Hands free

19.9.1. EMAS NHS Trust employees are not expected to use mobile telephones whilst driving. It is illegal to use a mobile phone held in the hand while driving or while stopped with the engine on. Any deviation from this policy is at the driver's own liability and no responsibility will be accepted by EMAS for such actions. [2]

19.9.2. EMAS can provide compatible hands-free kits upon request to the IM&T Department or EMAS Fleet Services.

19.10. **Camera**

19.10.1. Cameras on mobile telephone devices are enabled to support business functions. Breaches in confidentiality resulting from inappropriate usage will lead to disciplinary action. Please refer to section 18 for guidance on usage.

## 20. Device Management

20.1. All EMAS owned devices within the Trust are to be managed by the IM&T Department. This includes;

- Asset Management/Redistribution of devices
- Replacement for Lost/Stolen devices
- Procurement of new devices

20.2. If a user leaves EMAS employment (or in some cases moves to a different directorate), the mobile device is to be returned to the IM&T Department. IM&T will need to amend configuration records. Users do not have the right to 'pass on' equipment to other staff without prior approval from the IM&T Department.

## 21. Legislation

21.1. Users of Portable Devices must comply with current legislation regarding the use and retention of Patient information and use of devices. These include, but are not limited to:

- *The Data Protection Act 1998*
- *Access to Health Records Act 1990*
- *The Copyright, Designs and Patents Act 1988*
- *The Computer Misuse Act 1990*
- *Road Traffic Act 1988*

## 22. Sanctions

22.1. Any breaching of these policies and laws may result in disciplinary action being taken due to the far-reaching implications for the Trust of any non-compliance.

22.2. It is not non-compliance in itself that may lead to disciplinary action but the intent and consequences of that non-compliance.

[2] *The use of Airwave radio terminals are excluded from the scope of this policy; the use of which whilst driving is permitted under the Road Traffic Act 1988 (exemption from prosecution is stated for the use of an emergency service in a response scenario)*

22.3. Where fraud is suspected, the matter will be referred to the Trusts Local Counter Fraud Specialist for investigation in accordance with the Trusts Fraud and Corruption Policy.

## 23. Consultation

23.1. The IM&T Security Group has been consulted to ensure that all areas of access are reviewed or removed when a user moves or leaves the employment of EMAS.

23.2. The Information Governance Group (IGG) has been consulted to ensure that this policy mitigates risk to the Trust's information.

## 24. Monitoring, Compliance and Effectiveness of the Policy

24.1. The monitoring of this policy will be carried out by the IM&T Service Delivery Team on an annual basis.  Additional reviews will be undertaken if significant changes to services are identified prior to the standard review date.

24.2. The policy will be approved by the Information Governance Group as identified in the Trust's Scheme of Delegation.

Appendix 1

# Plan for Dissemination of Procedural Document

| | | | |
|---|---|---|---|
| **Title of document:** | **IM&T Portable Device Usage Policy** | | |
| **Version Number:** | **V4.0** | **Dissemination lead:**<br>**Print name, title and contact details** | **Steve Bowyer**<br>**Steve.@emas.nhs.uk** |
| **Previous document already being used?** | **Yes** | | |
| **Who does the document need to be disseminated to?** | **All EMAS staff** | | |
| **Proposed methods of dissemination:**<br>**Including who will disseminate and when**<br>Some examples of methods of disseminating information on procedural documents include:<br>*Information cascade by managers*<br>*Communication via Management/ Departmental/Team meetings*<br>*Notice board administration*<br>*Articles in bulletins*<br>*Briefing roadshows*<br>*Posting on the Intranet* | **Available on the Intranet**<br>**Chief Exec's bulletin**<br>**Inclusion in Policy advice list provided by Governance Team**<br>**Prior to release of IM&T Assets to end users** | | |

Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.

Appendix 2

Office Use Only

**CRN:**

## Portable Device Usage Policy - Acceptance Form

I have read and understood the Portable Device Usage Policy and IM&T Security Policy and I agree to abide by the requirements laid out by them and associated referenced policies.

Users Signature:

Date:

Please Print Name:

Department & Division:

Approved/Authorised by Name (in Caps):

Signature:

Date:

Portable Device Details/Description (If applicable please list mobile devices)

Make:

Model:

Serial Number:

IMEI Number (Mobile telephones & SIM Cards only):

EMAS Security Tag Number:

Mobile Telephone Number:

□ Car charger

------------------------------------------------------------------------------------------------------------------------

If applicable, please list any additional portable devices:

Make:

Model:

Serial Number:

IMEI Number (Mobile telephones & SIM Cards only):

EMAS Security Tag Number:

Mobile Telephone Number:

□ Car charger

------------------------------------------------------------------------------------------------------------------------