NHS
North Middlesex University Hospital NHS Trust

Telecommunications Policy

Policy Number	PO-000262
New or Revised Policy	Revised
Version:	5.2
Published:	16/09/2020
Review Date:	01/06/2023
Expiry Date:	**01/09/2023**
Policy Executive Owner:	Director of Finance
Policy Owner	Head of ICT
Policy Author/s	Head of ICT
Ratification Committee	Policies & Guidelines review and ratification group
Date ratified:	01/09/2020
Approval Committee:	Information Governance Emergency Planning Committee
Date approved:	26/08/2020
Target Audience:	All staff
Linked Policies:	Information Technology Security Policy Data Protection Policy. Safe Haven Faxes Procedures Clinical Photography and Video Policy Media Policy Wi-Fi policy Information Governance Assurance Management Framework Resilience and Response Policy Emergency Preparedness Policy Business Continuity – Telecommunications, Telephones and Bleep Systems Mobile Device E-mail Policy
Key Words:	Mobile, Bleep, Text, SMS, Telephone, VoIP, Analogue, smartphone, iPad, Tablets, Fax, Pager, Voice-mail, Handset, Mobile communication devices, Radio handset
Name of other committees & meetings consulted	Executive Management Board
Designation of Individual Staff Members or staff groups consulted	Head of Medical Equipment Management Unit Finance Department Switchboard Department.

This is a Controlled Document. Staff must refer to the Intranet version of this document to confirm the most up to date version of this policy. If older versions are in circulation, they must be either returned to the author above or destroyed.

Version and document control:

Version number	Date of issue	Author	Status	Change Description*
0.1	July 08	IT Services Manager	Draft	Circulated for comments
0.2	July 08	IT Services Manager	Draft	Added Telecommunications Engineer comments
0.3	July 08	IT Services Manager	Draft	Added Deputy Chief Executive comments
1.0	August 08	IT Services Manager	Final	Ratified by HMB
2.0	June 11	IT Services Manager		Policy review for discussion at IG Committee
2.1	June 11	IT Services Manager		Added IG Committee comments
2.2	June 11	IT Services Manager		Executive Management Board for ratification
3.0	August 11	IT Services Manager	Draft	Amalgamation of: Telecommunication Policy and Mobile Communications Devices Policy
3.1	September 11	IT Services Manager	Final	For ratification
4.0	May 14	Head of IT	Final	Policy review and reformatting
5.0	August 2017	Head of IT	Final	Policy review
5.1	August 2020	Head of Technology	Final	Policy Review

Contents

1. Introduction

1.1 North Middlesex University Hospital (NMUH) provides access to a variety of telecommunications services to enable staff to communicate effectively with each other, partner organisations and service users and to use other phone features for Trust purposes.

1.2 The Trust voice infrastructure consist of Avaya CS 1000, Siemens ISDX 3000 switchboards using a combination of Voice Over Internet Protocol (VoIP) and analogues telephones respectively.

1.3 This policy is aimed at promoting safe, proper and cost-effective use of voice communications equipment within the Trust, by its employees and any other individuals or groups authorised to use the equipment or systems belonging to the Trust. The policy covers desk telephones, facsimile, SIM enabled devices (i.e. tablets, laptops) and mobile voice communication devices (i.e. mobile telephones, smartphones, pagers and bleeps).

1.4 Non-compliance with this policy may result in disciplinary action, including dismissal and notification to the appropriate authorities of criminal or suspected criminal actions.

2. Purpose of the Policy

2.1 North Middlesex University Hospital NHS Trust is committed to ensure that telephone contact between Trust staff and other organisations or members of the public is conducted in a professional and efficient manner. For this reason there is a policy in place for the use of all telecommunication devices and for the making and receiving of telephone calls.

2.2 All staff should be made aware of the standards expected of them when using the telephone and of any additional departmental arrangements. These standards should be followed whenever the telephone is used; they apply equally to internal and external calls.

2.3 This policy is intended to create a framework of rules which will result in a safe working environment for all the staff involved with the treatment of patients, and for the patients who are being treated, by minimising risk of Electromagnetic Interference to the delicate medical devices from the use of Mobile Communication Devices. Mobile phones incorporate cameras and video recorders and this policy is also intended to create a legal framework to protect the privacy and dignity of all the patient of the Trust.

2.4 There are no specific regulations governing the safe use of Mobile Communication Devices. This policy references advice as listed in Appendix F.

2.5 The use of the any software application used on any devices covered within this policy including clinical applications such as Careflow Connect are out of scope of this policy.

3. Duties within the organisation

3.1 Senior Information Risk Owner (SIRO) ensures that appropriate policies are in place to ensure that telecommunication policy is adhered to across the Trust.

3.2 Caldicott Guardian ensures that patient information is kept confidential and used appropriately in line with Caldicott Principles.

3.3 Head of IT is responsible for the day-to-day management of the procedures related to this policy.

3.4 Divisional head of nursing, department managers will take the necessary steps to ensure compliance with this policy within their clinical areas.

3.5 It is the responsibility of all staff to ensure that patients, visitors and other staff comply with this policy. Anyone who does not comply potentially compromises the care of patients. Action will be taken to avoid such risks.

3.6 Switchboard is responsible for putting out crash calls upon notification. Switchboard is also responsible for calling the agreed staff members in response to a major incident as per the Emergency Preparedness, Resilience and Response Policy and Emergency Group Alert.

3.7 Non-sanctioned installations of telecommunications equipment or use of unauthorised equipment is strictly forbidden and may result in disciplinary action..

4. Definitions

4.1 Telephone: A device that permits two or more users to conduct a conversation when they are not in the same vicinity of each other to be heard directly.

4.2 Mobile Phone: A telephone that can make and receive telephone calls over a radio link while moving around a wide geographic area.

4.3 Smartphone: A mobile phone with more advanced computing capability and connectivity than a basic feature phone.

4.4 Voice Over Internet Protocol (VoIP) Phone: Uses VoIP technology for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional Public Switched Telephone Network (PSTN).

4.5 Analogue Phone: A handset that converts sound waves into an electrical signal for transmission across a phone system.

4.6 SIM Card: Subscriber Identification Module (SIM) is an integrated circuit that securely stores the International Mobile Subscriber Identity (IMSI) which is used to identify and authenticate subscribers on mobile telephony devices.

4.7 Text Messaging: A message composed on the phone and sent using the Short Message Service (SMS) over the mobile network.

4.8 Facsimile: A telephone transmission of scanned printed material (both text and images), normally to a telephone number.

4.9 Pager/Bleep: A device that receives and displays numeric or text messages, or receives and announces voice messages.

4.10 Voice-mail: A computer based system that allows users and subscribers to exchange personal voice messages.

4.11 Radio handsets/terrestrial trunked system – also known as walkie-talkie

5. Usage

5.1.1 Telephones owned by the Trust are restricted to business use only. International and premium rate calls are restricted. International and premium rate calls must be approved by the relevant Divisional Director, and must be made through the switchboard who will log the details.

5.1.2 To ensure that the Trust resources are used efficiently the current provision of the dial 9 for an external line will be regularly reviewed with a view to reducing the number of telephone extensions with this facility to a minimum. Members of staff that have a need to make an external call, whether business or private will need to arrange access to an extension with this facility via their line manager. Otherwise an external line can be provided via the switchboard by dialling 0 and call details will be recorded.

5.2 Personal Telephone Calls

5.2.1 The Trust recognises that there may be exceptional occasions, normally due to unforeseen circumstances, where it is necessary for members of staff to make personal telephone calls. Staff should be aware, however, that the making of or receiving of private telephone calls is not approved by the Trust and the use of the telephone system is, therefore, a privilege and not an automatic right. This privilege can be temporarily suspended or completely withdrawn on an individual or collective basis if circumstances indicate that this is appropriate.

5.2.2 When making or receiving a private telephone call staff should take account of the following points:

- Private calls (incoming and outgoing) should be kept to a minimum and be of short duration;
- Outgoing private calls should be authorised by the line manager and made through the switchboard where the operator must be advised that the call is private so that the call details might be recorded;
- Be aware that the Trust has deployed call logging (source, time, duration of call and destination) to analyse telephone usage, to deliver value for money, to highlight misuse, or breaches of telephone security, and will investigate any such activities reported, taking action, where necessary, to minimise the risk to the Trust;
- Ensure that the nature and content of private calls is appropriate to the business environment in which they are received;
- Note that it is unacceptable for staff to conduct regular private business or administration using the Trust telephone system. Such abuse of the Trust telephone system will result in the instances being considered to be of a fraudulent nature, which may lead to disciplinary or criminal action against that individual;
- Staff spending inappropriate amounts of time on the telephone, even if the call has not been made using the Trust system, (i.e. receiving private calls) is also an abuse of the Trust telephone system and could result in disciplinary action;
- Any suspicions of the fraudulent use of telecommunications equipment may be reported to your line manager or directly to the Local Counter Fraud service or NHS Fraud and Corruption Reporting line where calls will be kept in the strictest confidence and all staff are protected under the Public Concern at Work (Whistle blower) Act;

5.2.3 The onus of responsibility lies with the individual staff member to declare private use of the Trust telephone system. Where a member of staff does not declare private use and are found to have made use of these services without the appropriate permission they may be subject to disciplinary action.

5.3 Unauthorised Access

5.3.1 It is against Trust policy to attach any mobile computer (i.e. laptop, tablet, smartphone etc.) to the Trust telephone infrastructure without the approval of the Head of IT. Such abuse of the Trust telephone system will result in the instances being considered to be of a fraudulent nature, which may lead to disciplinary or criminal action against that individual.

5.4 Facsimile

5.4.1 The use of Facsimile (Fax) is prohibited by the Trust except in exceptional circumstances (e.g. loss of the Trust corporate E-mail service) or where the use has been agreed with the Head of Information Governance. Refer Appendix E Safe Use of Facsimile Machines.

5.5 Voice-mail

5.5.1 Subject to available licenses all Trust extensions are able to activate secure voice E-mail. This service can be set up by the user and details should be requested via the IT Services service desk. Voice-mail users should ensure:

- Their personal PIN is not disclosed to any other individual either within or outside the Trust;
- A current message must always be set when activated. Greeting messages are simple, short, are appropriate and give accurate information;
- Messages are actioned and cleared promptly;
- It is the responsibility of the user for the management of their voice mailbox.

5.5.2 Confidential messages regarding named individuals should not be left on voice-mail.

5.5.3 Any voicemail processes which involve leaving messages for patients and service must ensure that the confidentiality of patients is maintained. Clinical information must not be left on voicemail messages for patients and service users.

5.6 Payphones

5.6.1 The Trust will provide access to payphones where there is a requirement. The department requiring the payphone will be responsible for all rental and maintenance costs.

5.7 Incoming Calls

5.7.1 The use of auto attendant should be encouraged for all incoming calls where the extension number is known. This reduces the volume and thereby increases the speed with which calls can be answered by the switchboard operators.

5.8 Fault Reporting

5.8.1 All faults should be reported to the IT Services service desk.

5.9 Management of Trust Mobile Phones

5.9.1 This policy gives guidance on eligibility for Trust mobile phones and outlines users' responsibilities in connection with mobile phones issued.

5.9.2 Named data held on mobile devices such as address books, text messages and E-mails is subject to the same restrictions under the Data Protection Act and the Trust's Information Technology Security Policy, as all personal identifiable data held by the Trust, and so all mobile devices must as a minimum be password protected by a Personal Identifiable Number (PIN).

5.10 Criteria

5.10.1 Mobile phones are only allocated to staff meeting the following criteria and with the written agreement of their Divisional Director:

- The user works alone in situations that potentially may endanger personal safety;
- The user is based in the community;
- The user is required for on-call;
- The user is regularly in situations where security is an issue;
- The user is regularly away from their desk and need to be contacted quickly whilst at work;
- The user works away from the normal office location on a regular basis and must be able to be contacted to answer queries at short notice or has a need to obtain verbal advice from support staff.

5.10.2 A mobile telephone will not be procured for permanent use if:

- The user does not meet the above criteria;
- The user fulfils the requirements for issue of a mobile phone on a periodic basis only. For example, on maternity cover, the mobile held by the postholder should be used for this purpose.

5.10.3 Staff will be routinely issued with the current Trust standard mobile. Staff requesting a mobile phone with additional features to the Trust standard mobile (e.g. smartphone) must get the approval from the relevant Divisional Director. Staff will be issued with the current Trust standard smartphone model.

5.10.4 Request for the temporary use of a mobile device must be made to the IT service desk giving seven (7) days' notice by the Divisional Director.

5.11 Procedure

5.11.1 The relevant line manager should seek approval from the appropriate Divisional Director, giving the reason for eligibility. Once approval has been given, a call should be logged to IT Services service desk. A standard handset and SIM card will be ordered.

5.11.2 On receipt of the mobile phone, the user will be required to read and sign the Acceptance for the Use of Mobiles Phone by staff employed by North Middlesex University Hospital NHS Trust (refer to Appendix G).

5.12 Replacement Handset

5.12.1 Replacement handsets will only be provided when the handset cannot be repaired (i.e. normal wear and tear). Users who abuse or damage the equipment supplied to them will be required to fund its replacement.

5.13 Private Calls

5.13.1 Mobile phone users are permitted to make private calls from Trust mobile phones. However, the Trust must be reimbursed in full for all private calls made.

5.13.2 Users will be asked to verify private calls on their itemised bill. Payroll will deduct the agreed amount from users' salaries.

5.14 Safe-keeping of Handsets

5.14.1 Care should be taken for the safe-keeping of handsets:

- Users should keep mobiles secured and out of sight wherever possible;
- Access PIN numbers must be used;
- Patient telephone numbers should never be stored in the phone memory;

5.14.2 If a mobile is lost or stolen, the following action should be taken:

- Alert the IT Services service desk Ext 2345 immediately;
- IT Services request a bar to be put on the mobile to prevent calls from being made;
- Note log number for police report, if necessary;
- Report loss to line manager;
- Complete a Trust Datix Incident Form.

5.15 Return of Handset

5.15.1 Issued handsets remain the property of the Trust and must be returned to the line manager on leaving the Trust's employment. The line manager must return the handset to the IT Services department.

5.15.2 The Trust will seek to recover the cost of the handset, if this is not returned on departure, and any personal calls invoiced after the user has left the Trust's employment.

5.16 Mobile Phones General Use of Mobile Phones

5.16.1 It is illegal to hold and operate a hand held device whilst driving. Therefore the use of mobile phones or hand held device for Trust business whilst driving is strictly prohibited. No in-car mobile phone kits will be provided by the Trust.

5.16.2 Users should not make or answer calls whilst driving on Trust business. Users should switch their phones off before driving and read messages or return calls when safely parked with the vehicle engine turned off.

5.16.3 Users will be responsible for any fine or penalty incurred for breach of legislation if using a mobile device whilst driving. The Trust will not take responsibility or be liable in any way for staff charged with using a handheld device whilst driving and will not in any circumstances, contribute in any way to the payment of fines or other expenses incurred by use of a handheld device.

5.16.4 SIM cards must not be exchanged between mobile devices without the knowledge and approval of the Head of IT.

5.16.5 International roaming will be barred by default on all Trust mobiles devices. This bar may be lifted at the written request of the relevant Divisional Director.

5.16.6 Text messages exchanged within the context of Trust business and those exchanged using Trust supplied mobile telephone are part of the Trust corporate records and may be examined by Trust management if necessary and may be disclosable under the Freedom of Information Act 2000.

5.16.7 The transmission of Multimedia Messaging Services (MSM) will be barred by default on all Trust mobile devices.

5.16.8 Personal music and photographs must not be stored on smartphones.

5.16.9 Subscriptions by staff to text messaging services (e.g. sports results, new updates etc.) are prohibited from Trust mobile devices.

5.16.10 Personal Identifiable Data (PID) held on mobile devices (e.g. address books, text messages, E-mail etc.) is subject to same restrictions under the Data Protection Act as all other PID held by the Trust. All mobile devices are issued with a Personal Information Number (PIN). Users must not disable this feature.

5.16.11 Staff who holds smart phones must not store Personal Identifiable Data on the smart phone memory. Please refer to the Mobile Device E-mail Policy for further guidance.

5.17 Patient and Visitors Use of Mobile Phones

5.17.1 The Trust will ensure that patient care, privacy and dignity are not compromised by the inappropriate use of mobile communications equipment through its sites. It is recognised that an appropriate balance needs to be achieved which allows patients to keep in touch with relatives and friends, but controls the encroachment on quiet and privacy of other patients.

5.17.2 Patients' connected to any medical equipment, the patient and their visitor's mobile phone must be switched off or enable 'airplane mode' to eliminate any risk of electromagnetic interference to the medical equipment.

5.17.3 It is also important to prevent the taking of inappropriate photographs and videos, to protect the privacy and dignity of all the patients of the Trust.

5.17.4 In line with Trust Policy, photographs and videos shall not be taken anywhere on Trust premises without permission and consent.

5.17.5 In line with Trust Policy, making video calls in a way that means no other person can see any other patient, visitor or staff member is permitted. Communication with family and friends is an essential element of support and comfort for a patient admitted to hospital

5.17.6 Patient and visitors may record conversations – doing so can help reduce anxiety for patients trying to remember and understand what was said. It also allows them to share the information later with their loved ones and carers. As a matter of good

practice, the patient/service user should inform all the participants involved within the conversation and seek permission.

5.17.7 The Trust permits patients or visitors mobile phones to be charged via the mains power supply but no medical device should be unplugged in order to charge a mobile device and the use of the emergency power supply is prohibited.

5.18 Consultant, Clinical and Nursing Managers Use of Mobile Phones

5.18.1 Consultants, clinical and nursing managers are allowed to use their mobile phones, when used in the interest of patients. However they must ensure they keep their mobile phones muted (silent) in all general clinical wards and waiting areas.

5.18.2 Consultant, clinical and nursing staff:

- Can use their mobile phone within outpatient clinics and clinical ward areas, however they should give due consideration to those around them, preferably by going to a quiet area;
- Must avoid unintended breaches of confidentiality through any such telephone conversations, as they might be overheard by casual passers-by and other staff members in public areas;
- Must switch off their mobile phone, if they need to get closer than two (2) meters to a patient connected to medical equipment.

5.18.3 Must switch off their mobile phone or enable ‘airplane mode’, prior to entering into any of the following clinically critical areas:

- Intensive Care Unit (ICU) patients rooms and nursing station;
- Progressive Care Unit (PCU) patients bedside and nursing station;
- Special Care Baby Care Unit (SCBU) patient areas;
- Accident and Emergency (A&E) resuscitation cubicle;
- Radiotherapy treatment areas;
- Operating theatres and theatre recovery areas;
- Catherisation laboratory;
- X-Ray Rooms including CT Scan and MRI control room;
- Labour delivery rooms;
- Endoscopy rooms and recovery rooms;
- Pathlogy laboratories (offices excluded).

5.19 All Other Staff, Patients and Visitors Use of Mobile Phones

5.19.1 All other members of staff and visitors working within North Middlesex University Hospital, are allowed to use their mobile phones, as a resource for keeping in touch and making use of online resources however they should give due consideration to those around them, preferably by going to a quiet area.

5.19.2 All staff, patients and visitors, are able to use mobile devices to Accessing helpful information about their conditions – apps and digital services can support greater patient participation, inform joint decision-making, and allow patients to provide feedback on their outcomes and experiences.

5.19.3 All staff, patients and visitors, must comply with this Policy; in so much as they are applied to the use of mobile communication devices on Trust premises.

5.19.4 Any member of staff who is aware of anyone having their mobile communication device switched on or using it within the above clinically critical areas (section 6.18.3.) must request the person to switch off the mobile, enable 'airplane mode' or to leave the clinical area, unless the user is a consultant, clinical or nursing manager.

5.19.5 Patients and visitors are to be made aware of, and are required to comply with, the hospital policy.

5.19.6 All staff must abide by the policy and ensure this is communicated throughout their area of work and enforced.

5.20 Telephone Directory

5.20.1 All staff are responsible for the continued accuracy of their own telephone directory entry on the Trust Intranet. Failure to keep this entry up-to-date leads to wasted time by operators and colleagues, can lead to delays in locating key staff in an emergency and contributes to an unprofessional image of the organization for external callers.

5.20.2 The telephone directory can be updated via the Internet using create new staff facility.

6. Bleeps and Pagers

6.1 Issuing and Management of Internal Bleeps and External Pagers

6.1.1 All pagers are managed on behalf of the Trust by the IT Services Department who is responsible for maintaining accurate records of pager holders.

6.1.2 All bleeps are managed on behalf of the Trust by the Switchboard Manager who is responsible for maintaining accurate records of bleep holders.

6.1.3 Bleeps or pagers will be issued to staff who meet the following eligibility criteria:
6.1.4 Part of an on-call rota.

6.1.5 For staff who does not take part in an on-call rota, requests must be approved by the relevant Divisional Director. New bleep or pager holders will be asked to sign Terms and Conditions of Use (refer Appendix H).

6.1.6 Doctors leaving the Trust must hand back pagers to IT Services Department before departure. Failure by doctor to hand back the pager may result with deductions made from their salary.

6.1.7 Rota co-ordinators will provide in advance to switchboard copies of all junior doctors' on-call and shift rotas.

6.1.8 Clinical Directors are responsible for notifying medical staffing, who advise switchboard, of consultants on-call rotas in advance.

6.1.9 Changes to all rotas must be notified to switchboard by medical staffing so that appropriate people are contacted in the event of a major incident or emergency.

6.1.10 All communication relating to changes to rotas should be sent by E-mail to the Switchboard Manager.

6.2 Use of Bleeps and Pagers

6.2.1 Switchboard and IT Services will provide written instructions on how to use bleeps or pagers upon allocation. Bleeps are tested prior to allocation to ensure they are functional. Pagers are tested on an ad-hoc basis to ensure major incident response.

6.2.2 Bleeps must be kept on-site at all times. This is particularly important when doctors and consultants are on leave, in order to provide bleep cover for locums.

6.2.3 The temporary swapping of bleeps is not permitted. However, in the very rare situations where this is unavoidable this must be organised via the switchboard.

6.2.4 Pagers must be kept with the person at all times so that they are contactable in the event of a major incident or emergency.

6.2.5 Personal calls to all bleeps are not permitted under any circumstance as they could interrupt patient care.

6.2.6 The transfer of bleep numbers to colleagues bleeps (piggy-backing) is strictly forbidden as a bleep with several numbers could delay contact in an emergency and interrupt patient care.

6.3 Leavers

6.3.1 Bleeps and pagers remain the property of the Trust. Bleep or pager holders must return their device to the switchboard before leaving the Trusts employment.

6.3.2 Medical and non-medical staff will return their devices to their line managers who are responsible for returning the device back to the switchboard or the IT Services Department.

6.3.3 The Trust will pursue recovery of the bleep or pager or financial recompense in every case.

6.4 Maintenance of Bleeps and Pagers

6.4.1 All bleep and pager holders are responsible for checking that their device is in full working order at the start of their shift. Any fault with the bleep or pager must be reported to switchboard who will arrange repairs and provide a temporary replacement, wherever possible.

6.4.2 If the bleep or pager is sent off for repair belongs to an on-call doctor the bleep or pager number will be transposed to a spare device for the duration of the repair.

6.4.3 Switchboard will replace batteries in bleeps and pagers when required. Flat batteries should be reported to switchboard.

6.4.4 The bleep or pager holder is responsible for ensuring that batteries are replaced when flat.

6.4.5 Lost or stolen bleeps or pagers remain the responsibility of the holder who must report any loss immediately to switchboard or to the IT Services Department.

6.4.6 Where the Trust agrees to fund a replacement bleep or pager a budget code must be delivered to IT Services Department before a replacement can be purchased.

6.4.7 The costs of replacing any bleep or pager which has been damaged beyond economic repair must be met by the bleep or pager holder budget holder.

7. Radio Handsets

7.1.1 The Department of Health guidance of January 2009 gives reasons for not allowing the use of mobile phones in certain areas of hospitals. These are not solely related to interference with medical equipment.

7.2 Radio Handsets – North Middlesex University Hospital Personnel

7.2.1 These are mainly radio equipment used by hospital employees which have a high risk of causing Electromagnetic Interference (EMI) problems.

7.2.2 Risks could be minimised by use of alternatives such as pagers, cordless telephones or mobile phones. Otherwise consideration should be given to restricting the use of these radio handsets.

7.3 Radio Handsets – Emergency Services

7.3.1 These handsets are the most likely to cause interference problems, because of their higher power transmitters and lower operating frequencies. The following proposals have been agreed with the emergency services:

- Personnel carrying these phones should be made aware of the possible risks;
- Personnel carrying these phones should always make themselves known to hospital staff in charge of the area they are entering;
- Emergency service handsets should only be used in hospitals in an emergency, never for routine communications;
- Personnel should move well away from clinical areas before initiating or answering a call;
- Staff operating base stations should try not to contact an officer on routine matters while he or she is on hospital premises.

7.4 Mobile Data Terminals

7.4.1 These devices are frequently used by maintenance personnel on hospital premises to communicate with their office. The interference potential of the mobile data terminal system is between that of an emergency services radio handset and a mobile phone.

7.4.2 These Mobile data terminals should never be operated on or near any kind of medical device. Same restrictions apply as for the mobile phones usage within the hospital.

7.5 Radio Handsets – Terrestrial Trunked Radio System

7.5.1 These devices have some potential to interfere with medical devices, especially at short range. At longer range (distances greater than 2m) the risk is substantially reduced. This handset must not be used in areas listed in section 6.18.3.

7.6 Outside Media Broadcast Personnel

7.6.1 When outside media broadcast personnel come on to the hospital premises, the Trust's Head of Communications, or in his/her absence, a senior level representative of the hospital should:

- assist the Media personnel with the location and operation of their equipment;

- Inform the media personnel, who use radio handsets (radio-talkback system) on hospital premises, about the hospital's policy on the use of two-way radios for all locations in which they will be working;
- Ensure that any outside broadcast vehicles equipped with radio-talkback and microwave link transmitters, be parked and operated as far away as practicable from patient treatment areas or wards.

7.7 Outside Broadcast Vehicles

7.7.1 There are typically three main types of transmitting equipment likely to be used during outside broadcasts from hospital premises. These are:

- A Microwave link for the transmission of video data;
- A vehicle radio-talkback base station for onsite communication;
- Two-way radio handsets carried by broadcast staff also for onsite communication.

7.7.2 These broadcasting vehicles have the potential to cause interference to critical medical equipment, if operated near to patient treatment facilities. In order to minimise the risk, these vehicles should be parked as far away as possible from clinical areas.

7.7.3 The main risk of interference will be from the use of two-way radios carried by outside broadcast staff and used as part of the talkback system. The Trust senior level representative should make the Broadcasting staff aware of the Trust's policy on the use of the mobile radios in all areas where they will be working in.

8. Dissemination and Implementation

8.1 Following approval, this policy will be available on the Trust's intranet.

9. Process for monitoring compliance and effectiveness

9.1 The Trust will monitor compliance with this policy through regular audit and review and through monitoring the number and types of incidents related to E-mail and Internet use.

Criteria	Measurable	Lead	Frequency	Reporting to	Action–plan monitoring
Application of Procedures	Internal Audit	SIRO	Annually	Information Governance Group	IG Group
Incident Reporting	Datix Reporting	Head of PS&Q	Quarterly	Information Governance Group	IG Group
Induction Training	LMS Report	Deputy Director for Learning and OD	Quarterly	Information Governance Group	IG Group

10. References and Associated Documents

- Electromagnetic Compatibility of Medical Devices with Mobile Communications MDA DB9702 published in March 1997 by MDA.

- Mobile Communications: Interference with Medical Devices MDA SN9706 published in April 1997 by MDA.

- Emergency Service Radios and Mobile Data Terminals: Compatibility Problems with Medical Devices MDA DB1999(02) published in May 1999 by MDA.

- Update on Electromagnetic Compatibility of Medical Devices with Mobile Communications: TETRA (Terrestrial Trunked Radio System) and Outside Media Broadcasts from Hospital Premises MDA SN2001(06).

- Using mobile phones in NHS hospitals, January 2009 by DOH (Gateway 9768).

- Information Technology – Security techniques - BS ISO/IEC 217002: 2005.

- https://www.nhsx.nhs.uk/covid-19-response/data-and-information-governance/use-mobile-devices-patients-hospitals-eg-phones-tablets-and-cameras/

- https://www.gov.uk/government/publications/electromagnetic-interference-sources/electromagnetic-interference-sources#mobile-phones

11. Appendices

Appendix 1- Equality Analysis

Equality analysis is an evidence based approach which enables the Trust to have **due regard** to the need to eliminate discrimination, advance equality of opportunity and foster good relations, as required by the Public Sector Equality Duty (Section 149 of the Equality Act 2010).

Equality analysis involves gathering and analysing evidence to determine the possible impact of proposed policies, procedures and practices on different groups protected from discrimination by the Equality Act 2010 and then using such evidence to inform action to maximize positive impact and remove or minimize negative impact.

Equality analysis is required when:

- Developing a new policy or procedure
- Amending or reviewing an existing policy or procedure
- Commissioning a new service
- Reviewing delivery of a service

Equality analysis should be a meaningful exercise not a tick box process. Evidence of how the trust has had due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations can be requested to be made public.

In advance of implementing a policy please complete this template:

Division/Department:	**ICT , COR**
Name of person completing the equality analysis	**Head of ICT**
Date of Equality Analysis:	**Aug 2020**

What is the aim of this policy or procedure?	This policy is intended to create a framework of rules which will result in a safe working environment for all the staff involved with the treatment of patients, and for the patients who are being treated, by minimising risk of Electromagnetic Interference to the delicate medical devices from the use of Mobile Communication Devices. Mobile phones incorporate cameras and video recorders and this policy is also intended to create a legal framework to protect the privacy and dignity of all the patient of the Trust
Who will be affected by this policy or procedure? e.g. staff, patients, carers etc	All Staff
Is the policy/procedure being developed or reviewed?	Reviewed

Could this policy or procedure affect people differently because of:	**Yes/No**	**Is the difference likely to be positive or negative?** Please explain why	**What evidence sources have you used to make this assessment?*** Say if you have not used any evidence sources**
• Age	No		
• Disability	No		
• Gender Reassignment	No		
• Marriage/Civil Partnership	No		
• Pregnancy / Maternity	No		
• Race	No		

Could this policy or procedure affect people differently because of:	**Yes/No**	**Is the difference likely to be positive or negative?** Please explain why	**What evidence sources have you used to make this assessment?*** Say if you have not used any evidence sources**
• Religion or belief	No		
• Sex	No		
• Sexual Orientation	No		

* E.g. patient/staff surveys; patient/staff demographics; research (Local/national); borough/STP data; consultation exercises, management reports etc

** a lack of evidence should not be taken as a reason for stating that there is no impact on equality

12. Where you have indicated there is a negative impact on any group, could this be potentially discriminatory? * **	Yes/No If yes, could any discriminatory impact be objectively justified ****?
Where negative impact has been identified please say what action you will take to remove or mitigate this? Consider who will do this, by when and what the review arrangements there will be	

***** If you have identified a potential discriminatory impact of this policy/procedure please contact the Associate Director of Equality, Diversity & Inclusion or the Deputy Director Human Resources for advice.**

**** Is this a 'proportionate means of achieving a legitimate aim?' (cost alone is not sufficient justification)

Appendix 2 – Patient & Public Safety Impact Assessment Tool

Division: Corporate	
Policy/Strategy/Service redesign: Telecommunications Policy	
Lead: Head of ICT	
Date of Assessment: Aug 2020	
Review Date: Aug 2023	
Domains	**Impact of Policy, Strategy or Service Redesign on Patient Safety (Positive or Negative)**
Patient Safety	**Patient safety is one of the Trust's top priorities. This policy has been assessed for its potential impact on patient safety in July 2017.**
Mortality	**N/A**
Patient Experience	**N/A**
Staffing Levels	**N/A**
Quality of Service	**N/A**
What has been done to promote patient safety in this piece of work?	
Signature:	
Date:	

Appendix 3 - Safe Use of Facsimile Machines

All staff are reminded that facsimile (fax) machines should be used as a last resort when sending patient information.

The use of secure E-mail (nhs.net to nhs.net) or other secure government E-mail addresses is a much safer way of sending confidential information. If you don't know what is a secure government E-mail look for the following in the E-mail address:

.x.gsi.gov.uk	.gsi.gov.uk	.gse.gov.uk	.gsx.gov.uk
.pnn.police.uk	.cjsm.net	.scn.gov.uk	.gcsx.gov.uk
.mod.uk			

You may also ask the IT service desk about encrypting E-mail contents before sending if the recipient does not have a secure E-mail system.

If the use of a fax machine is unavoidable, the NHS Secure faxing principles must be practised at all times:

- Any confidential information held by the organisation should only be sent by fax where it is absolutely necessary;
- Patient identifiable information should only be sent by fax, in emergency situations;
- Ensure that fax machines are located in secure areas at both ends of the transmission;
- Always double check the fax number that you are sending information to;
- If you are unsure about the number you are sending a fax to, do not send the information without verifying the number with the recipient;
- Use pre-programmed numbers where possible to avoid misdialling;
- Contact the recipient before sending to let them know you will be sending a fax;
- Ask the recipient to acknowledge receiving the fax immediately;
- Confidential faxes must not be left lying around for unauthorised staff to see;
- Personal details should be faxed separately from clinical details. Clinical details should be sent; using the NHS number and no Patient identifiable Information should be within the detail;
- Make sure the fax cover sheet is marked Private and Confidential and states whom information is for.

For further information or advice contact:

Dr Achim Schwenk, Caldicott Guardian and Deputy Medical Director. E-mail: a.schwenk@nhs.net

Or Robert Ginter, IT Security Officer. E-mail: robert.ginter@nhs.net

Appendix 4 - Guidelines for the use of mobile / smartphones issued to NMUH employees

1. Introduction

These guidelines cover the use of mobile telephones and smartphones issued to employees by the Trust for use whilst on duty. This phone has been made available to you in order to:

Promote safe-working practices, i.e. if you are not returning to base at the end of a working day, you are able to contact somebody in the team to let them know, call emergency services should an emergency situation arise, etc.

Facilitate ease of contact between team members.

Facilitate ease of access by people outside of the team, i.e. switchboard, hospital departments, general managers etc.

Reduce the need for you to use patients' phones, outside call boxes and personal mobile phones in connection with your work.

These guidelines do not apply to individually owned mobile / smartphones used for Trust business. Reimbursement of rental for these is subject to the same criterion as for land line rental laid down by Agenda for Change (i.e. there must be a requirement to be contactable out of hours) and is reimbursed up to the equivalent of BT standard rental charge.

2. Condition of Use

This mobile phone / smartphone is provided for the sole use in connection with your work with North Middlesex University Hospital NHS Trust.

This phone / smartphone should not be used for personal calls. The cost of any personal calls made must be paid for and will be charged at invoice cost, plus 10%, plus VAT. It is the member of staff's responsibility to highlight this usage with the Manager and arrange for the cost of personal calls to be paid for.

All phones / smartphones will have a bar on usage outside of the United Kingdom, WEB browsing, premium rate numbers, directory enquiries and GPRS.

Members of staff will be requested to sign for the phone / smartphone. This will then be their personal phone and number. Once signed for, the member of staff becomes responsible for the phone's safe keeping and security. For example:

- Not to be lent to or borrowed by any person – colleagues, family etc.
- Not to be left exposed on front seat of car, or other vulnerable areas.

If lost or stolen the member of staff must report to the IT Services service desk immediately.

Members of staff are asked to use landlines where possible, e.g. in NHS properties.

Members of staff are reminded that use of a mobile phone / smartphone whilst driving is against the law, dangerous practice and therefore is not authorised by the Trust.

The manager will have monthly access to details of all phone usage and you will be asked to declare any private calls and will be charged for these. Managers will check the business calls for any unusual patterns of usage and will need to satisfy themselves that they are the Trust's liability. Audits within teams of phone usage will be undertaken on a random basis.

Members of staff will be responsible for returning their mobile phone / smartphone to the telecommunications engineer on leaving employment from North Middlesex University Hospital NHS Trust and must obtain a receipt for its return, which they should retain.

The member of staff will be asked to sign to say they agree to abide by this policy before being issued with a mobile phone (refer to Appendix G).

Appendix 5 - Acceptance for the Use of mobile / smartphone by Employees of NMUH

I have received and accept responsibility for the described mobile phone / smartphone*. I have read and received a copy of the guidelines and agree to abide by them.

Mobile / Smartphone * Number:	Network Supplier:
Sim Card Number:	Model:
Serial Number:	Connection Date:
Budget Code:	IT Reference Number:

Delete as appropriate

Name: Job Title:

Signature: Date:

Department:

Telephone Number: Divisional Director Name:

Appendix 6 - NMUH Pager / Bleep Acceptance Form

(a) This pager / bleep are the property of PageOne / Stanley and are leased to North Middlesex University Hospital NHS Trust.

(b) The user is responsible for its condition and whereabouts. If loss or damaged is caused to the pager / bleep, the user will be responsible for the replacement or repair cost.

(c) The user will notify IT Services Department should they leave the post, or hand the device onto another user.

(d) Department On-call pagers / bleeps are the responsibility of the Department Manager.

(e) The pager / bleep will be tested and the carrier must respond to these tests.

(f) The pager can be recalled at any time by the Telecommunications engineer, on instructions from the Trust.

(g) The user is to regularly test the pager to ensure that it is functioning correctly. Users must undertake to check their pagers at the beginning of every shift by paging themselves. Batteries may be obtained from the Switchboard. Switchboard must be informed if a pager is not functioning and advise switchboard of alternative arrangements or if appropriate obtain a temporary bleep/pager from switchboard.

(h) The maintenance of the pager will be overseen by the IT Services Department and it must be handed into switchboard if there are any problems with the device from where it can be returned to the supplier for repair or exchange.

User Details

Name:		Telephone:	
Job Title:		Extension:	
Department:		Manager:	

Pager Details

Pager / Bleep Number:	
Model:	
Serial Number:	
IT Reference Number:	

I have read and understand the above. I agree to abide by this policy and am fully aware of the serious problems and disciplinary action that could occur if these guidelines are not followed. I agree to deductions being made from my salary in the event of loss or damage to the pager / bleep that was due to my lack of care.

I hereby accept delivery of the above pager / bleep:

Name:		Date:	
Signature:		Job Title:	