North Middlesex University Hospital NHS Trust

Information Technology Security Policy

Policy Number	PO-000213
New or Revised Policy	Revised
Version:	5.2
Published:	10/10/2022
Review Date:	14/04/2025
Expiry Date:	14/07/2025
Policy Executive Owner:	Chief Finance Officer
Policy Owner	Chief Information Officer
Policy Author/s	Head of Technology
Ratification Committee	Policy Monitoring & Ratification Group
Date ratified:	04/10/2022
Approval Committee:	IT Steering Group
Date approved:	14/07/2022
Target Audience:	All staff, patients and visitors
Linked Policies:	Encryption Policy Data Protection Policy Internet & E-mail Access Policy Health Records Policy Registration Authority Policy Remote Access Policy Wireless Access Policy Telecommunication Policy
Key Words:	Information Governance, Information Security, Encryption, Security, Account, Network, Internet, E-mail
Name of other committees & meetings consulted	
Designation of Individual Staff Members or staff groups consulted	Head of Information Governance CCIO

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.

CONTENTS

VERSION CONTROL SHEET

Version	Date	Author	Status	Comment
0.1	1 Jul 09	IT Services Manager	Draft	First Draft
0.2	13 Jul 09	IT Services Manager	Draft	For Comment
0.3	20 Jul 09	IT Services Manager	Draft	Changes following comments
0.4	21 Jul 09	IT Services Manager	Draft	For discussion and approval by Data Protection and Security Sub-Committee – 28 Jul 09
1.0	28 Jul 09	IT Services Manager	Final	For ratification by HMB – 21 August 2009
1.0	21 Aug 09	IT Services Manager	Final	Ratified by HMB 21 August 2009
1.1	7 Dec 09	IT Services Manager		Network and E-mail accounts addendum – For ratification by HMB 18 Dec 09
1.2	Sept 10	IT Services Manager		Amendments
2.0	Aug 11	IT Services Manager		Policy review
3.0	Oct 13	Head of IT	Final	Policy review
4.0	Sept 15	Head of IT/IT Security Officer	Final	Policy review
5.0	Feb 19	Head of IT Services	Draft	Policy Review
5.1	April 2019	Head of IT Services	Draft	Revision following ITSG comments
5.1.1	April 2019	Head of It Services	Draft	Formatting and inclusion of comments for DS and appendix 4 circulated as separate document
5.2	July 2022	Head of Technology	Final	Approved at IT Steering

CHANGES & ALTERATIONS TO CURRENT POLICY (For revised policies only)

- Changes to job titles and committee names throughout
- Clarification of position regarding use of NUMH systems to store personal data (section 13)
  Inclusion of Cyber Essentials Plus standard (sections 1 & 9)
- Inclusion of ransomware, malware, phishing (section 3)
- References made to Divisional Triumvirates / Heads of Service (section 11)
- Added reference to record keeping of trained individuals (section 21)

QUICK GUIDE TO INFORMATION SECURITY

- **All staff are to use complex passwords which are changed on a regular basis (maximum of 90 days).**
- **Password should never be disclosed (this includes to other Trust computer account holders).**
- **All workstations should be locked or logged off when unattended.**
- **All staff should be cautious about any potential SPAM/unsolicited emails and delete any at the earliest possible opportunity.**
- **No staff are to connect privately procured hardware to any Trust computing equipment or network without prior written approval from the IT Department.**
- **Only IT staff are to install any software on Trust computing equipment**
- **All IT facilities must be used responsibly and staff must understand the terms of acceptable usage.**
- **All IT assets (including equipment, software, information, and infrastructure) are Trust property and are entered on the Trust's IT asset register maintained by the IT Department.**
- **The disposal of redundant equipment is the responsibility of the IT Department including the secure disposal of media holding and/or having stored personal information.**
- **All proposed changes to the Trust IT infrastructure and services (e.g., software upgrades/installations and new IT services) must gain approval of the IT Strewing Group and Change Advisory Board (CAB) before implementation.**
- **Staff are to comply with the General Data Protection Regulations (GDPR), The Data Protection Act 2018, and Caldicott Principles, never disclosing any Trust information or provide access to such information to unauthorized recipients or those who do not "Need to Know".**
- **Staff should expect no privacy when using the corporate network or trust resources; such use may include but is not limited to transmission and storage of files, data, and messages.**
- **Any member of staff observing an IT Security incident must raise a report in accordance with the Trust Risk Management Process (i.e., via Datix) and provide the IT service desk with relevant details.**
- **IT Security is an integrated part of Information Governance (IG) and all staff must undergo IG training on an annual basis.**
- **Information security principles apply equally to mobile and remote devices (refer to the Trust's Mobile Device Policy)**

1. Introduction

1.1. It is the responsibility of all NHS organizations to maintain effective information security, and all NHS bodies are now mandated to adopt the Information Security Standard: BS ISO/IEC 27001:201327007:2013 (International Code of Practice for Information Security Management) and the Information Security Management: NHS Code of Practice.

1.2. The Trust will take the necessary steps to become compliant with the national Cyber Essentials Plus standard

2. Purpose of the Policy

2.1 The purpose of this Information Technology (IT) Security Policy is to protect, to a consistently high standard, all information assets, including patient's records and other North Middlesex University Hospital Trust (NMUH) corporate information, from all potentially damaging threats, whether internal or external, deliberate, or accidental.

2.2 Its purpose is to identify and address security management in the processing and use of NHS information and is based on current legal requirements, relevant standards, and professional best practice.

2.3 This policy will achieve a comprehensive and consistent approach to the security management of information throughout NMUH, thus ensuring continuous business capability, and minimize both the likelihood of occurrence and the impacts of any IT security incidents.

2.4 The policy sets out the arrangements required in all processes associated with scanned records in order to reduce the risk of a challenge to the legal admissibility and evidential value of the scanned records. The key objectives are to preserve:

2.5 Confidentiality – Access to data must be confined to those with specific authority to view the data.

2.6 Integrity - Information is to be complete and accurate. All systems, assets and networks must operate correctly, as per agreed specifications.

2.7 Availability – Information must be available and delivered to the right person, at the time when it is needed.

2.8 The policy applies to full-time and part-time employees of the Trust, non-executive directors, contracted third party organizations and individuals (including agency staff), trainees, seconded, apprenticeships, volunteers and other staff on placement with the Trust and staff or partner organisations with approved access.

2.9 Where there is evidence of a breach of the policy, it will be investigated and acted upon in accordance with the Trust disciplinary procedures. In such cases the Trust reserves the right to disable users' account and deny access to such equipment or impound equipment.

3.0 Risk Assessment

3.1 Threats to the system are assessed under three main types of threats:

3.2 Physical (e.g. theft, damage, water damage, fire damage etc.): these are mitigated by the existing IT security measures to the data centres. Scanners housed in the scanning bureau will have the same security measures applied, as per Trust security, and health and safety policies.

3.3 Technical (e.g. ransomware, malware, phishing, Denial of Service attacks and failure to function) Access to the scanning bureau and records storage areas are controlled using Trust access control devices (i.e. swipe cards). Business Continuity Plans are currently being developed for the system both from the scanning bureau and operational user's perspectives.

3.4 Personal: all staff must be trained to use systems according to their role and access. Standard operating procedures will be in place for all to follow. The Trust's Information Governance Policies and Confidentiality Code of Conduct apply, and all staff who has breached policies is subject to disciplinary action in line with the Trust's disciplinary policy and procedures.

4. Duties within the organisation

4.1 The policy applies to full-time, part-time employees of the Trust, non-executive directors, contracted third party organisations and individuals (including agency staff), trainees, seconded, apprenticeships and other staff on placement with the Trust and staff or partner organisations with approved access.

4.2 Where there is evidence of an offence it will be investigated and acted upon in accordance with the Trust disciplinary procedures. In such cases the Trust reserves the right to disable users' account, deny access to such equipment or impound equipment.

5. Consultation and Approval

5.1 **Consultation and Communication with Stakeholders**

5.2 The following were consulted during the writing of this policy:

- Head of Information Governance
- Caldicott Guardian
- Chief Medical Information Officer
- IT Security Officer
- Informatics Team
- Data Quality Team
- Medical Device and Equipment Management Team

6. Responsibility for Document Development

6.1 This policy is developed by the Head of Technology and monitored by the IT Steering Group The Executive Lead is the Chief Finance Officer / SIRO.

7. Development of the Policy

7.1 Equality Impact Assessment

7.1.1 The Equality Act 2010 became law in October 2010 and covers the same equality strands that were protected by previous equality legislation, but extends some protections to groups not previously covered, and also strengthens particular aspects of equality law. It replaced previous legislation (such as the Race Relations Act 1976 and the Disability Discrimination Act 1995) to ensure consistency in what employers need to do to make an organisation compliant with the law.

7.1.2 This policy was screened for impact on equalities in November 2010. As a result of this screening, it has been decided that a full equality impact assessment is not required. Please refer to Appendix 3 for the Equality Assessment Screening Tool.

8.0 Patient Safety Impact Assessment

8.1 Patient safety is one of the Trust's top priorities. This policy has been assessed for its potential impact on patient safety in October 2013 and again in 2019. The Patient Safety Impact Assessment can be found in Appendix 3.

9.0 Scope and Definitions

9.1 The guidance contained within the NHS Code of Practice and its related materials applies to NMUH information assets of all types. Refer to Appendix b

9.2 The Trust will take the necessary steps to become compliant with the national Cyber Essentials Plus standard

9.3 The Trust must be compliant with the Data Security and Protection Toolkit. DSPT

10.0 Prioritisation of Work

10.1 North Middlesex University Hospital NHS Trust needs robust information security management arrangements for the protection of key information services. This policy ensures that:

- Information is properly protected and is readily available to properly authorised personnel as and when it is required.
- Relevant regulatory and legislative requirements shall be achieved.
- The integrity and evidential value of information shall be maintained.

11.1 Roles and Responsibilities

11.2 Chief Executive

11.2.1 The Chief Executive has overall responsibility for IT Security in the Trust. This responsibility must be discharged through a designated member of staff who has lead responsibility for IT security management within the organisation.

11.2.2 The information security lead must be of appropriate seniority e.g. Board level or reporting directly to a Board member. This lead role must be formally acknowledged and made widely known throughout the organisation. The Chief Finance Officer is the Trust's SIRO and is accountable to the Board for all information risks and mitigation.

11.2.3 The Senior Information Risk Owner provides assurance to the Trust Board that all information security risks have been identified and appropriate mitigations are in place.

11.2 Chief Information Officer

11.2.1 The Chief Information Officer has lead responsibility for the IT Security at a strategic level within the Trust.

11.2.2 The CIO has responsibility for escalating all IT Security concerns to the Trust Board and advising on Level of Risk/Issue and mitigating actions

11.2.3 The CIO has management responsibility for the Head of Technology who manages the day to day IT Security processes and policy implementation

11.3 Head of Technology

11.3.1 The Head of Technology has responsibility for the management of IT Security operational processes within the Trust. This includes:

- Understanding what information is held
- Knowing what is added and what is removed
- Understanding how information is moved
- Knowing who has access and why

11.3.2 Escalates security concerns to the Trust Board via the CIO

11.3.3 Is responsible for reporting IT Security incidents to the CIO and IT Steering Group and Information Governance and Data Security Steering Group

11.3.4 With the Head of Clinical Engineering, providing assurance to the IT Steering Group, the Information Governance Steering Group, and executive team on the effective management and handling of Care CERT notifications of threats from NHSD

11.3.5 With the Head of Clinical Engineering, providing assurance to the IT Steering Group, the Information Governance Steering Group and executive team, of the safe disposal of any devices holding PID

11.3.6 With the server and network team within IT, the CIO, and the Head of IG, responsible for ensuring relevant levels of encryption are used to secure information and data are protected

end-to-end across the internal networks internally and with any authorised external connections via HSCN.

11.4 Head of Information Governance

The Head of Information Governance has responsibility for:

11.4.1 Ensuring appropriate notification in compliance with the Data Protection Act 2018 and GDPR 2016 is maintained for The Trust's information.

11.4.2 Dealing with enquiries about information governance issues and facilitating subject access requests.

11.4.3 Advising and training staff on their information governance responsibilities.

11.4.4 Advising on actual or potential breaches of confidentiality and recommending remedial action.

11.4.5 Ensuring the Trust has an action plan for achieving compliance with the requirements of the Data Security and Protection Toolkit ensuring The Trust has procedures in place to comply with relevant Department of Health best practice guidance such as Confidentiality code of practice and Records Management code of practice.

11.4.6 Liaising with external organisations on information governance matters

11.4.7 The development and implementation of information sharing protocols.

11.4.8 The Information Security Officer, Head of IT and the Head of Information Governance will work collaboratively to ensure that the Trust has a data security improvement plan. The implementation of the plan will be overseen by the Data Security and Cyber Security Group and reported to the Data Protection and Security Sub-Committee.

11.4.9 As the Data Protection Officer, the CIO is the Trust's main link to the Information Commissioner's Office

11.5 Information Technology Security Officer

The Information Technology Security Officer has responsibility for:

11.5.1 Implementing, monitoring, documenting and communicating IT security within the Trust, in compliance with United Kingdom legislation and national policy and guidance.

11.5.2 Monitoring and reporting the state of IT security within the Trust to the Head of Technology and the CIO.

11.5.3 Liaising with the Information Governance and Data Security Steering Group over the IT security input to the Data and Cyber Security Forum and IG agenda.

11.5.4 Liaising with relevant senior, line and system managers over information security.

11.5.5 Liaising with the Head of IT Services over information security at the operational level.

11.5.6 Management of the CareCERT process and auditing of its effectiveness and providing relevant reports for IT Steering, Data and Cyber Security Forum and IG Group

11.5.7 Ensure this IT Security Policy is implemented and followed throughout the Trust.

11.5.8 Ensure relevant staff are aware of their security responsibilities and that security awareness training is provided for all users.

11.5.9 Ensure that IT system users know how to report any security breaches, incidents, malfunctions and suspected system weaknesses and threats.

11.5.10 Monitoring for actual or potential information security breaches within the Trust Caldicott Guardian/CCIO

11.6 The Caldicott Guardian

The Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information The Caldicott Guardian is responsible for:

11.6.1 Ensuring all current and future staff are instructed in their security and National Data Guardian recommendations responsibilities.

11.6.2 Education of all current and future staff on protection of patient-identifiable data in electronic and non-electronic data use.

11.6.3 Ensure that exchange of patient-identifiable data within the Trust and with outside persons/agencies follows the Caldicott Principles.

11.6.4 Ensure that procedures are in place for role based access, and monitor the application of such procedures. The Caldicott Guardian must sign off all RBAC for systems which process patient data.

11.7 Divisional Triumvirates / Heads of Service

Divisional Directors and Heads of Service are information asset owners for the information assets held within their divisions and departments, and as such are responsible to ensure the security of the data held within.

11.7.1 Divisional Directors and Heads of Service have responsibility for:

11.7.2 Ensuring all their staff undertake IG & Data Security statutory and mandatory training on an annual basis.

11.7.3 Ensuring all staff are instructed in their security and information governance responsibilities.

11.7.4 Ensuring all staff using computer applications are trained in their use.

11.7.5 Ensuring unauthorised staff is not allowed to access any of the Trusts computer applications.

11.7.6 Determining which individuals are to be given authority to access specific computer applications. The level of access to specific systems must be on a job function need, independent of status.

11.7.7 Regularly reviewing the authority and level of access given to users to ensure it still reflects their job function needs and is independent of status.

11.7.8 Implementing procedures to minimise the Trusts exposure to fraud, theft, and disruption of its systems.

11.7.9 Ensuring current documentation is always maintained for all critical job functions to ensure continuity in the event of individual unavailability.

11.7.10 Ensure staff is aware of the Trust Standing Orders and policy on potential personal conflicts of interest.

11.8 All Staff

All staff:

11.8.1 are personally responsible for undertaking their annual statutory and mandatory Information Governance update

11.8.2 are personally responsible for ensuring that no breaches of computer security result from their actions.

11.8.3 Must not disclose their password or allow anyone else to use their password or allow other users to work under their user account.

11.8.4 Staff issued with a smartcard must not divulge the pass code, nor share their smartcard with any other user. They must take steps to ensure that the security of the smartcard is maintained at all times.

11.8.5 Must comply with the Trust's relevant IT and confidentiality policies and procedures.

11.8.6 Understand that breaches of policy will be investigated by formal disciplinary procedure which may lead to dismissal and/or legal action.

11.8.7 are personally responsible for the accuracy and currency of the data they record on systems.

11.8.8 Must declare any potential conflicts of interest as required by The Trust's Standing Orders.

11.9 System Managers

11.9.1 Job descriptions for system managers will include specific reference to the security role and responsibility of the post.

11.9.2 All Trust's systems must have at least two individuals with the expertise to administer the particular system.

11.9.3 All Trust's critical computer systems (i.e. those which have a direct impact on patient care or have a business critical function) must have at least three individuals with the expertise to manage or administer such a system.

11.10 Head of Clinical Engineering

11.10.1 Responsible for holding up to date relevant asset register for Medical Devices and equipment with embedded hard drive devices

11.10.2 Responsible for liaising with Medical Device and Equipment manufacturers regarding the application of any relevant operating system patches and upgrades in line with CareCERT notifications from NHSD

11.10.3 Working with the Head of Technology and the IT Security Lead to identify, action and report back completion of relevant remedial actions to maintain system and network security

11.10.4 Responsible for identification of hard drives within Medical Devices that will contain PID and liaising with the IT Services department for the safe removal and disposal of Hard Drives before any such Medical Devices are decommissioned and removed from site

11.10.5 Ensuring relevant Medical Device and Equipment contracts with suppliers, address the need for information security associated with PID on embedded Hard Drives/devices and appropriate handling of removal and replacement of parts

11.11 Other Authorised Users

Other NHS and authorised external users:

11.11.1 Are personally responsible for ensuring that no breaches of computer security result from their actions.

11.11.2 Must comply with the Trust security policies and procedures.

11.11.3 Shall have this policy referenced as part of a relevant service level agreement or contract together with the appropriate confidentiality statement.

12 Risk Management

12.1.1 Threats to the Trust data shall be appropriately identified and based upon robust risk assessment and management arrangements.

12.1.2 All systems will be subject to periodic security reviews by the IT Services Department conducted using the Information Governance (IG) Toolkit and with reference to ISO/IEC 27001:2013. The depth of a review will be determined by the importance and size of the particular system. IT security and information governance must link directly with the Trust's risk management process.

The Trust must ensure that it has a documented plan and programme that considers the security risks to all its information assets.

12.1.3 All IT security incidents will be formally logged, using the Trust Incident reporting system.

12.1.4 Information Security incidents will be reported by the Information Security Officer to the Data Security and Cyber Security Working Group and the Information Governance and Data Security Steering Group. Both the Quality and Audit Committees will receive regular reports on all aspects of information governance from the Information Governance and Data Security Steering Group.

13 Security of Data

13.1 Data must not be stored on users' local Personal Computer (PC) hard drives or removable devices. If Personal Identifiable Data is to be saved it must only be on network drives and the transfer of data using USB ports will be disabled

13.2 Encrypted removable devices may only be used with specific permission of the Head of Technology or the Head of Information Governance

13.3 Members of staff or users who are authorised to use Trust PCs are not permitted to save any personal data or non-Trust business related material (e.g. word, excel documents, photo images, music, video files) on the Trust network storage devices or local hard drives. The IT Department will undertake routine audits of all file servers and the Trust reserves the right to remove and destroy any such material without consultation or notice.

13.4 Acquisition and storage of inappropriate materials e.g. pornography or offensive or criminal material is strictly forbidden and is deemed a disciplinary offence. At the recommendation of the Head of technology, in consultation with the Deputy Director of HR, the user's account may be disabled pending the outcome of investigations.

13.5 Only users authorised by the Head of Technology will be issued with Trust approved encrypted USB sticks for the storage of Trust data, or have the ability to write to CD or DVD. Where CDs or DVDs are used, they will be encrypted and require password protection.

13.6 Person Identifiable data must not be saved to any removable media. If this is absolutely necessary for business purposes, the removable media must be encrypted to the required NHSD specification (256-bit encryption.)

13.7 To maintain the integrity all central systems will have daily backup regimes formalised in the appropriate job run. Back-up schedules and documentation are held by the Head of Technology – access to the documents is restricted to highly sensitive nature of the information.

13.8 Secure storage will be used for the backup media. Such storage must be geographically separate from the data center locations to protect against building loss.

13.9 All CareCERT notifications from NHSD will be managed according to the documented Process

13.10 The Head of Technology will ensure that a penetration test is conducted annually. The scope of the penetration test will be agreed with the CIO, the Head of Information Governance and approved by the SIRO at the Information Governance and Data Security Steering Group.

13.11 Hard drives from IT (including printers and or Medical Devices will be retained and destroyed by an approved supplier, with relevant certification for safe and secure destruction, before leaving the Trust site).

13.12 End to end encryption of information and data transmitted across the network should be implemented where technically possible

13.13 Loss of Trust IT equipment and mobile devices MUST be reported immediately to the IT Helpdesk and any associated potential for data breech reported to the Head of Information Governance

13.14 The use of cloud services will be permitted only after due diligence has been completed and a Data Protection Impact Assessment has been conducted, reviewed by the DPO and all risks mitigated.

14 Software Protection and Standards

14.1 To comply with the law on licensed products and minimise risk of malicious software all users must ensure that they only use licensed copies of commercial software.

14.2 All IT software must be purchased through the IT Services department.

14.3 It is a criminal offence to make or use unauthorised copies of commercial software; offenders are liable to disciplinary action, civil or criminal prosecution.

14.4 Measures will be in place to detect and protect the network from viruses and other malicious software.

14.5 Users must report all viruses detected or suspected on their PCs, laptops, tablets, phones etc. immediately to the IT Services service desk.

14.6 All clinical applications must be supported by relevant supplier support/maintenance agreement

14.7 All relevant CareCERT remedial actions notified by NHSD will be applied where technically possible. Where not possible technically, the risks associated with this must be escalated to the Data and Cyber Security Forum, IG Group and IT Steering Group

15 Equipment Location and Protection

15.1 Equipment must be sited to reduce risks from environmental threats, and from unauthorised access. Where equipment must be kept in public areas, it must be positioned to reduce the risk of unauthorised access or casual viewing. Environmental controls will be installed to protect central and key equipment. Such controls will trigger alarms if environmental problems occur. In such cases only authorised entry will be permitted.

15.2 The Trust's data centres / server rooms are high security areas housing its servers, data and voice equipment. An entry restriction and intruder detection system will be incorporated to protect the data centres.

15.3 Unrestricted access to the central computer facilities will be confined to designated staff, whose job function requires access to that particular area. IT Services may give restricted access to other staff and third party support where a specific job function demands such access.

15.4 Data and voice communications network equipment and N3/HSCN terminating equipment must be located in secure areas in lockable cabinets.

15.5 All central processing equipment, including servers, will be covered by appropriate support and maintenance agreements. All PCs, laptops and printers will be covered by maintenance agreements with third parties for repair of out of warranty equipment provided it is cost effective (each case will be judged on its merits). All such repairs will only be made on approval by the IT Service Department. All such third party individuals involved in the maintenance of IT equipment will be required to sign and abide by confidentiality agreements. Records of all faults will be maintained by the IT Services Department.

15.6 Critical computer and network equipment will be fitted with battery back-up, using Uninterruptible Power Supplies (UPS), to ensure it does not fail during switchovers between mains

and generator. These UPS units must provide sufficient power to ensure, where technically possible the relevant system(s) can be shut down gracefully in the event of supply generator back-up not being available. Where a system is not manned continually, where technically possible, management software must be installed to allow the automatic shutdown of the system in the event of a power failure.

15.7 All cabling (electrical or communications) between buildings will, where practical be via underground conduit not accessible to unauthorised people. All cabling within buildings will be in conduits if surface mounted, otherwise within the framework of the building. Suitable cable trays will be used for computer cables and these will be sited in accordance with the relevant standards in relation to electrical and heating services. All cable installations will be carried out using industry best practice and relevant standards.

15.8 Drinking and eating are strictly forbidden and the use of mobile phones or other radio- frequency devices are discouraged in areas housing computer and network equipment. Warning signs to this effect must be prominently displayed within these areas, but not on the outside of doors or entrances to secure areas.

15.9 Where computer systems are located in areas that could easily be accessed by unauthorised staff, (e.g. clinical offices, wards and reception areas), extra care must be taken to leave unattended computers in a safe, and password protected state.

16 Information Asset

16.1 Information assets may consist of:

- Digital or hard copy patient health records (including those concerning all specialties and General Practitioners (GP) medical records).
- Digital or hard copy administrative information (including, for example, Personnel, estates, corporate planning, supplies ordering, financial and Accounting records).
- Digital or printed clinical diagnostic images, slides and imaging reports, outputs and scanned copies.
- Digital media (including, for example, data tapes, CDs, DVDs, USB disc drives, USB memory sticks and Medical Device embedded Hard drives e.g. in Scanners AND Printers).
- Computerised records, including those that are processed in networked, mobile or standalone systems.
- E-mail, text and other message types.

17 User Access Control, audits and Passwords

17.1 The Trust will ensure that user access controls are in place to control individual's access to systems to that required by their job function.

17.2 The Trust will ensure that all systems are auditable by user access and activity; queries criteria should be enabled to respond to queries either by user or by activity.

17.3 Formal procedures will be used to control access to systems. IT application forms must be fully completed and countersigned on receipt by the IT department.

17.4 All users are required to sign the Acceptable use of Information Systems prior to being granted access to Trust systems

17.5 All accounts that have not been accessed for a period of ten (10) months will be suspended, and after a further two (2) months without any request for reinstatement the account will be deleted.

17.6 Access privileges will be modified or removed, as appropriate, when an individual changes job or leaves the Trust.

17.7 No individual will be given access to a live system unless properly trained and made aware of his or her security responsibilities.

17.8 Passwords must be at least ten characters long. Users must keep their passwords secret, never disclose them to colleagues. The sharing of password(s) is a disciplinary offence.

17.9 Passwords must be changed at least every ninety (90) days. All new systems must include password ageing to force users to change their password.

17.10 Network components must have their default passwords changed and the Head of IT will provide confirmation that this has been undertaken on an annual basis.

17.11 It may be necessary occasionally to access a member of staff network or E-mail account (e.g. if a member of staff is unexpectedly away for an extended period) or for the purposes of investigations Requests must be made in writing by the staff member's manager to the Head of Technology. The authorisation must be countersigned by the CIO or a relevant Executive Director.

17.12 Under exceptional circumstances generic accounts will be set up. This must be authorised by an executive director using the normal Network Application forms.

18 Remote Diagnostic

18.1 Suppliers of central systems expect to have remote access to such systems on request to investigate faults. The Trust will only permit such access subject to N3/HSCN and Statement of Compliance (SOC) security requirements being achieved. Any supplier requiring remote access will be required, before access is granted, to provide a written commitment to maintain confidentiality of data and information and only use qualified representatives. The written commitment can be contained within a signed commercial contract which contains the appropriate Data Protection Clauses or a stand-alone agreement. (Appendix 5) Each request for remote access will be authorised by the IT Services Manager. Modem links will not be connected.

18.2 Virtual Private Network (VPN) allows users with the appropriate authority to connect to the Trust data communications network from a remote location via the Internet.

19 Business Continuity Planning

19.1 The Trust recognises that if some form of disaster occurs the IT Department must seek to contain the impact of such an event through tested business continuity plans. The Trust recognises that IT systems are increasingly critical to its business and that the protracted loss of key systems/user areas could be highly damaging in operational terms. The Trust requires tried and tested business continuity plans for its computing facilities to be maintained.

20 Asset Inventory

20.1 An up-to-date register of acquisitions and disposals of physical computer assets (e.g. servers, PCs, Printers etc.) will be maintained by the IT Services department and presented twice yearly to the Information Governance and Data Security Steering Group.

20.2 An up-to-date register of all proprietary software will be maintained by the IT Services department together with relevant license conditions.

20.3 The IT Services Department will ensure that IT equipment and data storage devices are irreversibly purged of data before they are securely destroyed and documented using the Trust Asset Disposal Form. This includes the disposal of Hard Drive Disks within printers, scanners and Medical devices

20.4 The Inventory of Medical Devices will be maintained by the Head of Medical Equipment Management Unit and this must include reference to devices with embedded hard drives. The Head of MEMU will present the inventory of Medical Devices with the accompanying information security information e.g. embedded hard drives, interfaces etc. to the Cyber and Information Security Forum twice yearly.

21 Training and Education

21.1 No individual will be given access to a live information system unless properly trained and made aware of their security responsibilities. Information security training is covered during mandatory staff induction.

21.2 Training in use of any computer system must include the security of that system.

21.3 Relevant information security training and awareness will be available to all staff.

21.4 Where possible provision for a suitable Training environment should be provided

21.5 Records of individual trained must be kept, either in an IT department database (in the case of departmental systems or resulting from the introduction of new systems), or in Phoenix, the Trust's learning management system (in the case of key clinical systems such as EPR or EPMA)

21.6 Access to key clinical systems such as EPR or EPMA will not be granted until the relevant training has taken place and can be evidenced

22 Policy Approval

22.1 The policy will be presented for approval at the IT Steering Group, the Information Governance and Data Security Steering Group and ratified by Policies Ratification Group.

23 Dissemination and Implementation

23.1 This policy will be available on the Trust's intranet.
23.2 This Policy will be communicated and discussed with the Operational Management Group

24 Process for Monitoring Compliance and Effectiveness

24.1 The Trust will monitor compliance with this policy through regular audit and review and through monitoring the number and type of incidents related to information security.

Criteria	Measurable	Lead	Frequency	Reporting to	Action-plan monitoring
Application of procedures	Internal audit programme	SIRO	Annually	Audit Committee	Information Governance and Data Security Steering Group
Data Security and Protection Toolkit	Compliance Audit annually	Head of IG	Quarterly	Audit Committee	Information Governance and Data Security Steering Group
Incident Reporting	Datix report	Data Security Lead	Quarterly	Audit Committee	Cyber and Data Security Forum

25 Key Performance Indicators

The implementation of this policy will be audited by the Data and Cyber Security Forum, reported to the Information Governance and Data Security Steering Group.

26 References – Legislation and Best Practice Guidance & References

Access to Health Records Act 1990

The Human Rights Act 1998

Electronic Communications Act 2000

Regulation of Investigatory Powers Act 2000

Health & Social Care Act 2001

Data Protection Act 2018

Copyright Patents and Designs Act 1988

Computer Misuse Act 1990

Public Records Act 1967

NHS Code of Practice – Information

NHS Code of Practice – Records Management

Security Management

BS ISO/IEC 27001:2013:2005 (International Code of Practice for Information Security Management)

NHS Code of Practice – Confidentiality

Department of Health - The Caldicott Committee

BS ISO/IEC 27001:2005 (International specification for the Information Security Management System ISMS)

Common Law Duty of Confidentiality

Freedom of Information Act 2000

Civil Contingencies Act 2004

Appendices

Compulsory appendices:
Appendix 1 - Equality Assessment
Appendix 2 - Patient Safety Impact Assessment Tool

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:	**IT**
Name of person completing the equality analysis	**Richard Bowyer**
Date of Equality Analysis:	**July 2022**

What is the aim of this policy or procedure?	The purpose of this Information Technology (IT) Security Policy is to protect, to a consistently high standard, all information assets, including patient's records and other North Middlesex University Hospital Trust (NMUH) corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental
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	N/A	Not used any evidence sources
• Disability	No	N/A	
• Gender Reassignment	No	N/A	
• Marriage/Civil Partnership	No	N/A	
• Pregnancy / Maternity	No	N/A	
• Race	No	N/A	
• Religion or belief	No	N/A	
• Sex	No	N/A	
• Sexual Orientation	No	N/A	

* 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

Where you have indicated there is a negative impact on any group, could this be potentially discriminatory? * **	**N/A**
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	N/A

***** 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 Safety Impact Assessment Tool

Division: IT	
Policy/Strategy/Service redesign: Redesign	
Lead: Brendan Mahony, Chief Information Officer	
Date of Assessment: October 2022	
Review Date:	
Patient Safety Domains	**Impact of Policy, Strategy or Service Redesign on Patient Safety (Positive or Negative)**
Mortality	**Positive – by protecting the integrity of the Trust IT Infrastructure and Network, patient information at the point of care is enabled to support relevant decision making and therefore potential positive impact on mortality**
Patient Experience	**Positive – by protecting the integrity of the IT infrastructure, the integrity and availability of patient information is supported to allow for more efficient delivery of patient care and handling of enquiries**
Staffing Levels	**Positive – by protecting the IT Systems and Data, the staff experience is more positive and retention possibly at a higher level. By making access to information more resilient by reducing incidents of downtime associated with data and network security issues, staff are able to be more efficient**
Quality of Service	**Positive – protecting data and systems against potential threats it is possible to support a more robust quality of service**
What has been done to promote patient safety in this piece of work? Protection of privacy and integrity of personal information	
Signature: 	
Date: 04/10/2022	