Policy Document

Reference: IT02

NHS
University Hospitals of North Midlands
NHS Trust

Personal Information Security and Acceptable Use

Version:	**2**
Date Ratified:	**January 2019 by Trust Executive Committee (TEC)**
Date of Next Review:	**January 2022**
Expiry Date:	**January 2023**
Policy Author:	**Information Security Manager**
Executive Lead:	**Director of IM&T / SIRO**

Version Control Schedule

Version	Issue Date	Comments
1	November 2017	
2	January 2019	Inclusion of DPO roles and responsibilities Updating of wording and dates to reflect GDPR Updating wording to Data Protection Impact Assessments Updating safe email guidance to reflect local changes Include details about Apps and Trust or personal data

Statement on Trust Policies

The latest version of ‘Statement on Trust Policies’ applies to this policy and can be accessed here

CONTENTS **Page**

1. INTRODUCTION

Over recent years, the NHS has turned to the use of modern IT systems to enable it to improve the quality, safety and efficiency of services it delivers to patients, delivery partners and the public. Central to this is the requirement for NHS organisations to have in place robust IM&T Security controls to ensure the protection of patient information and compliance with regulation.

With the introduction of the Information Governance Assurance Framework, the NHS has become accustomed to delivering an incremental improvement programme, designed to steadily improve information management and information technology risk management. Performance against this framework is now routinely built into Trusts audit cycles, used by NHS regulators such as the Care Quality Commission and NHS Improvement and forms part of the evidence base for the Information Commissioners Office should they come and review how a Trust is complying with the Law.

Whilst the costs of the NHS getting it wrong continue to increase, with 2 NHS organisations fined a total of £365,000 for inadvertently publishing special categories of personal data and staff information in 2016 alone, the threats and consequences of external Information Security threats to UHNM continue to evolve:

- There have been the high-profile, global cyber incidents such as Gameover, ZeuS and Cryptlocker, which between them have defrauded over half a million people worldwide of millions of pounds; or the more recent attacks on Sony Pictures which resulted in the leaking of sensitive data as well as a number of the studio’s unreleased films; and the increasing appetite of criminals to target healthcare organisations who, like UHNM, rely on their information and information systems to support the delivery of patient care.
- Then there are those attacks closer to home, that might not result in the big headlines, but which nevertheless are hugely damaging, both to the UK economy and individuals. The BIS 2014 Information Security Breaches Survey reported that 81% of large organisations had experienced a security breach of some sort. This costs each organisation, on average, between £600,000-£1.5 million and in some cases, the organisation was so badly damaged by the attack that they had to change the nature of their business

Whilst it is vital that UHNM have in place technical controls to protect itself from external and internal threats, it is also vital that the users of the Trusts IM&T resources understand their Information Security responsibilities.

This policy, which outlines the responsibilities of all Trust IM&T users, forms part of the Trusts overall Information Security Management System, designed to support compliance with:

- Data Protection Act and GDPR
- Regulation of Investigatory Powers Act 2000
- Equality Act 2010
- Human Rights Act 1998
- Civil Contingencies Act 2004
- NHS Information Governance Framework
- ISO: 27001 Information Security Management Standard

This policy should be read in conjunction with:

- ICT06 Trust Guidance on Sending Personal Identifiable/Sensitive Information by E-Mail
- IT07 Trust Policy for Information Security Management
- IT08 Email and Internet Policy
- IG04 Trust Safe Haven Policy
- IG07 Information and Governance Management Framework and Policy
- RM01 Risk Management Policy and Strategy
- RM07 Management of untoward Incidents including Serious Untoward Incidents

- RE01 Multidisciplinary Health Records Policy
- RE02 Clinical Photographic and Video Policy
- IG08 Freedom of Information Act Policy
- G11 Corporate Records Management Policy
- G09 Trust Policy for the Management, Protection and Disclosure of Employment Related Information
- HR53 Statutory and Mandatory Training Policy
- HR01 Disciplinary Policy and Procedure
- HR17 Trust Policy for Induction Training

Where more in depth documentation is available in other documents this is indicated in each section.

2. SCOPE

This policy forms part of an Information Security Management System, which is designed to protect the availability, integrity and confidentiality of the University Hospitals of North Midlands NHS Trust (UHNM) information and information systems.

This policy covers the acceptable use Standards for Personal Information Security and Acceptable Use - expected of **All** UHNM Employees using UHNM IT resources in terms of the following:

- Incident Management
- Physical Security
- Clear Desk and Clear Screen
- Secure Disposal
- Passwords and Pass codes
- Malware (Virus)
- Mobile Devices and Remote Working
- E-Mail and Internet Use
- Social Media Use

The purpose of this policy is to detail the information security requirements that all individual employees must follow in order to protect the information assets owned and used by UHNM from threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements.

All individual members of staff will be required; to sign up to this policy through the Standards for Personal Information Security and Acceptable Use agreement at Appendix A and this acceptance will be recorded for audit purposes.

In additional line managers will be required to sign up to the additional line mangers requirements at Appendix B.
Any staff afforded enhanced rights on any IT systems will also be required to sign up to the additional requirements at Appendix C.

This policy's aim is not to impose unnecessary restrictions but rather to ensure that all UHNM employees are fully aware of the rules surrounding the use of this policy and to enable them to make appropriate use of information assets.

Compliance with this policy is mandatory for all employees. This policy forms part of the terms and conditions of the contract of your employment – breach of the rules in this policy will result in disciplinary action being taken against you which could lead to your dismissal. Misuse of IM&T resources or breach of this policy could also lead to civil or criminal actions against you or UHNM.

3. DEFINITIONS

Anonymisation	The process of anonymisation involves the removal of personal identifiers from a dataset to minimise the risk of disclosure. Data which is "truly anonymised" contains no information that could be used, by anyone, to identify the individual whose data it is.
Back Up	Retained copies of data, programs, operating systems and configuration. Usually for disaster recovery and contingency purposes.
Cloud or remote storage	A model of networked online storage where data is stored in virtual pools of storage hosted by third parties. Hosting companies operate large data centres, to which their customers can store files or data objects. Physically, the resource may span across multiple servers, sites or even countries.
Confidential	'Information of a confidential nature' or 'confidential information' means any information relating to UHNM patients, carers, clients, partners, vendors, the internal affairs of UHNM business or UHNM employees.
Cyber Crime	Criminal activity / crime which involved the internet, a computer system or computer technology. This includes but is not limited to crimes such as identify theft, phishing or hacking.
Data	The computer term for information, mainly used for information that is processed, stored or transmitted in computerised forms.
Encryption	A method of scrambling data, either at rest or in transit, to ensure that it cannot be understood without an additional password, key or other security measures.
File	A file is simply a recording of information. A complete collection of related data is a file.
Hardware	The physical equipment - electronic, mechanical, magnetic and other components such as memory, peripherals, terminals, disk, power supplies. Examples include PCs, laptops, printers and USB sticks.
Internet	The Internet is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. Information stored, accessed or transmitted via the internet should not be

	viewed as private or secure.
Log On/Sign On	A method of enabling the computer to recognise a user by the user entering a name and password.
Log Off/Sign Off To	A procedure for exiting/quitting the computer program in a safe and controlled way.
Malware (Virus)	Malware, or malicious software including: • Computer viruses - A piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users. • Phishing – usually an email appearing to come from a trusted source that is seeking to illegally extract passwords, usernames or other identity information to allow unauthorised access to the Trusts network and/or systems • Ransomware – a specific type of virus becoming more common, which encrypts your data and requires payment for a key to unencrypt it – i.e. it holds the organisation to ransom. • SPAM – unwanted e-mails that clog up storage and are often used as a means to infect IM&T resources with a virus. E-mail attachments and Internet sites are the most common method of infection; however it is still common for virus infection to occur from media being copied onto a PC.
Network	A network consists of two or more computers linked together for the purpose of sharing information and/or peripheral devices.
Person Identifiable Data (PID)	Those items of data concerning a data subject that, if used singly or in conjunction with other data items, could lead to identification of the data subject. Data items include Name, Address, Photographs and Clinical Images, telephone and email contact details.
Pseudonymisation	Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers in a consistent manner so that patient specific activities can still be grouped but against the now unknown patient Pseudonymised Data is not the same as Anonymised Data. When data has been pseudonymised it still retains a level of detail in the replaced data that allows the organisation that pseudonymised

	to re-identify activity back to the original patient if needs be. Care must be taken to ensure the keys to the unencryption of activity is not shared with recipients
Removable Devices	Peripheral devices usually associated to data storage (USB sticks, external hard drive, zip drive etc.).
Network Area Storage	Large central servers or collections of servers managed by IM&T which provide secure storage space for users.
Secure VPN	A dedicated network connection between 2 points or more where the data flowing over the network is encrypted using a network device at each point.
Special Categories of Personal Data	Those items of Personal Identifiable Data consisting of information about - the racial or ethnic origin of the data subject, their political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), their physical or mental health or condition, their sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

4. ROLES AND RESPONSIBILITIES

Chief Executive

The Chief Executive has ultimate corporate responsibility for Information Security and Information Systems.

Director of IM&T

The Director of IT has day to day strategic responsibility for IT and Information Systems. The Director is also responsible for ensuring that the Trust's information systems, computers, networks and devices, have the necessary security to ensure that its information (that needs to be kept confidential) remains confidential. Further, that data has the necessary integrity and that data and systems are available as necessary.

Managers

All Trust Managers are responsible for ensuring that their members of staff:

- Receive Information Security education and training
- Are aware of their responsibilities for Information Security

Specific responsibilities for Managers can be found in Appendix B of this Policy

Information Security Manager

Responsible for maintaining this and other associated policies and procedures and providing specialist guidance. The Information Security Policy and associated procedures shall be maintained, reviewed and updated by the information security manager with review taking place annually or more frequently in response to major events or legislation or governance changes.

Information Governance Manager
A senior representative in the organisation who is a specialist and leads and co-ordinates the information governance development programmes. The key purpose of this role is to ensure the Trust successfully reports on and manages the risks associated with information governance; to ensure the establishment of corporate standards which achieve legal and ethical compliance legislation with all elements of information governance.

Caldicott Guardian
All NHS organisations must appoint a Caldicott Guardian which is a role that is an amalgamation of management and clinical issues, helping to ensure the involvement of healthcare professionals in relation to achieving improved Information Governance compliance. The Caldicott Guardian has responsibility for ensuring that all staff conforms to the Caldicott Principles and the guidance contained in the NHS Confidentiality Code of Practice. The Caldicott Guardian (CG) will guide the Trust on confidentiality and protection issues relating to patient information. This role is pivotal in ensuring balance between maintaining confidentiality standards and the delivery of patient care. The CG will also advise the Trust Board on progress and major issues as they arise. The Trust’s Caldicott Guardian is the Medical Director.

IT Clinical Risk Lead
In line with ISB standard DSCN18 the Trust is required to have an IT Clinical Risk Lead, who must report to the Trust’s Clinical Governance lead. This role ensures that relevant risk management processes are followed to minimise any risks to patient safety in respect to the deployment and use of software products. The IT Clinical Risk Lead must be independent rather than part of any IT or Project team.

Senior Information Risk Owner
It is a mandatory requirement that the Trust nominate a Senior Information Risk Officer (SIRO). The nominee should be an Executive Director or Senior Manager to be responsible for the ownership of information risk across the Trust and to undertake the role of SIRO. The SIRO will be expected to appreciate how the Trust’s strategic business goals may be impacted by information risks and the links with risk management and information governance. The SIRO is strategically responsible for Information Security and Information Risk across the Trust. The Trust’s SIRI is the director of IM&T.

Data Protection Officer (DPO)
The DPO is responsible for:

- Informing and advising UHNM on Data Protection regulations, and national law or Data Protection provisions;
- Ensuring the alignment of this policy with Data Protection regulations, national law or Data Protection provisions;
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Acting as a point of contact for and cooperating the Information Commissioners office and the relevant Data Protection Authorities (DPAs);
- Making and keeping current notifications up to date with the Information Commissioner’s Office;
- The establishment and operation of a system providing prompt and appropriate responses to Data Subject requests;
- Informing senior managers, officers, and directors of UHNM of any potential corporate, civil and criminal penalties which may be levied against UHNM and/or its Employees for violation of applicable Data Protection laws;
- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
- Provides Personal Data to UHNM
- Shares personal data with UHNM
- Processes personal data for UHNM
- Ensure that the Trust notification and registration is maintained and kept up to date

- Raise awareness of and promote the General Data Protection Regulations and the Data Protection Act
- Provide advice to staff at all levels
- Liaise where appropriate with the Data Protection Officer from the relevant Trusts, Local Authority and Police etc;
- Ensure clear lines of accountability to the board on Information Governance & Data Security and Protection (IG & DSP) including monitoring the Trusts performance;
- Ensure that resources are available to support the IG & DSP Framework and Policy;
- Ensure that the Trust Board is briefed on IG & DSP and effectively supported and that there is appropriate access to expertise across all the elements of IG & DSP;
- Monitor breaches and recommend appropriate action;
- Providing a focal point for the resolution and/or discussion of IG &DSP issues.

Information Asset Owners and Staff with enhanced IT security privileges
Information Asset Owners are routinely responsible for locally managed information system are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they are responsible for.

Enhanced or Privileged access levels is defined as a levels of access above that of a normal user, this can include super user, power users, local admin, system administrator or simply access to records which would not normally form part of your role – e.g. the ability to view patient records whilst you are not clinically involved in that patients care.

Normal end users are protected, by inbuilt system controls, from carrying out actions that would endanger the availability, integrity or confidentiality of data held within Trust systems. Those with enhanced rights do not have these same protections in place, it is therefore vital that in order to protect both the information and this group of users, that appropriate access is clearly defined, recorded, and monitored.

Specific responsibilities for this group of staff can be found at Appendix C.

Privacy Officer
This is not a separate job title but is a role undertaken by the Registration Authority Manager. The role focuses on ensuring privacy related alerts from electronic systems (e.g. Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary.

All Staff
This policy applies to all employees of the Trust, Governors, Volunteers, other NHS and Health organisations, and other contracted staff, Partner Organisations and temporary staff, having the facility to use the Trust's e-mail and internet services, plus anyone granted access to the Trust network whilst engaged in work for the Trust at any Trust occupied location, and/or on any Trust owned or Trust approved computer or via remote access.

Compliance with this policy is mandatory for all employees. This policy forms part of the terms and conditions of the contract of your employment - breach of the rules in this Policy will result in disciplinary action being taken against you which could lead to your dismissal. Misuse of IM&T resources or breach of this Policy could also lead to civil or criminal actions against you or UHNM.

SPECIFIC INFORMATION SECURITY RESPONSIBILITIES FOR ALL STAFF

Incident Management

It is the responsibility of all employees to report security incidents. Information Security incidents should be reported to the IM&T Service Desk, to your Line Manager and should also be logged on DATIX in accordance with:

- RM01 Risk Management Policy and Strategy and

- RM07 Management of untoward Incidents including Serious Untoward Incidents -

The Information Security Manager will then ensure an investigation takes place.

All serious incidents relating to breaches of staff or patient data must also be escalated to the relevant divisional governance manager and the IG team.

Information security incidents include;

- Physical security breaches of UHNM premises
- Loss of UHNM owned information
- Loss or theft of UHNM Assets
- Malware (Virus)
- Misuse of UHNM systems
- Breaches of Laws
- System crashes
- Unlawful or inappropriate disclosure of staff or patient data

Physical Security

All offices should be secured at the end of each day. The keys for these offices should be stored in such a way as to maintain security. Designated key holders are responsible for the protection of office keys, and for the protection of the confidentiality of alarm codes. All UHNM employees are responsible for abiding by the following access rules:

- Ensure that visitors who you are responsible for sign in upon entry to offices and ensure they display a visitor badge.
- Chaperone visitors while they are within office premises until they leave or are handed over to another member of staff.
- If you recognise a person to be a non UHNM member of staff who is not chaperoned within UHNM premises politely ask them who they are visiting and ensure they are signed in, presented with a visitor pass and placed with the relevant member of staff.
- If you are the last member of staff to exit UHNM premises at the end of the working day ensure you abide with the relevant office exit procedure for locking premises securely.

Information Technology (Hardware) Asset Management

In order to comply with a variety of NHS requirements and its legal obligations, the Trust is required to know what Information Technology assets it holds, including:

The numbers, type and location of all IT hardware

- The software it uses
- The location of its data

To allow UHNM to comply with such obligations, all employees have a responsibility for abiding with the following rules:

- You must not move IT hardware such as PCs and Printers – You must notify IT Services if your IT equipment needs to be re-located and they will manage this for you
- You must not reallocate IT hardware assigned to an employee or worker if they change role or leave UHNM employment – You must notify IT Services of any such hardware
- You must not install or attempt to install software on UHNM IT hardware
- You must not attempt to connect any non-Trust devices to the Trust network.
- You must not upgrade or attempt to upgrade software on UHNM IT hardware
- You must not store UHNM information or data on non-UHNM devices such as USB Drives
- Unless it is part of a process agreed with the UHNM Information Governance Lead, you must not store UHNM data on cloud storage facilities (for example Drop Box, One Drive and Google Drive)

- You must not store UHNM or personal data on local computer disk (ie the C: Drive) use your personal and divisional mapped drives ie P: Drive.

Information Asset (Information System) Management.

All Information Assets (IT systems) in the Trust are recorded in a register, and each Information Asset must have a registered Information Asset Owner who is responsible for completing the required documentation suite and reviewing annually, this includes;

- A Data Protection Impact Assessment – on initial development or procurement or any change to how data is handled.
- A System Level Security Policy
- Risk Assessment
- Disaster Recovery and Business Continuity Documentation
- Data Flows Audit
- Information Sharing Agreement where required

No Information Assets must be developed, secured or otherwise procured (including FOC) without the express approval of the IM&T Information Security Forum.

Guidance on Information Assets, for example, types of data, data flows and legitimate sharing agreements can be found in IG07 Information Governance Management Framework and Policy and supporting Information Asset guidance.

Clear Desk and Clear Screen

UHNM operates a clear screen and clear desk policy. All UHNM employees are responsible for abiding by the following rules:

- Information of a confidential nature should not be available for casual viewing or inspection by visitors to UHNM offices.
- All confidential information including patient related documentation, personal identifiable information should be secured out of sight when a work area is unattended.
- Workstations should not be left unattended in a state where unauthorised individuals could access applications or documents. UHNM staff should ensure that PC's or other devices are screen locked when left unattended; this can be achieved by using the CTRL+ALT+DELETE or WINDOWS+L keys on desktop and laptop devices or by using the screen lock process in place for other tablet or smart phone devices.

Secure Disposal

Loss or theft of hard copy information or hardware poses a significant risk to UHNM. All UHNM employees are responsible for abiding by the following rules:

- All confidential documents must be shredded using a cross cut shredder (not a straight cue shredder or placed in a Trust confidential waste bin when ready for disposal. Under no circumstances should confidential information be disposed of in the rubbish bins or waste paper recycling units. Confidential waste bins are available for all areas.
- All confidential documents that have been sent to a shared printer should be collected straight away and not left on top of printers for casual viewing or inspection.
- Disposal of IT hardware assets must be arranged with IM&T who will dispose of it with due regard to legal requirements (software compliance, data protection and environmental regulations) and will ensure that the appropriate hardware and software registers are updated in line with NHS Policy - If a UHNM hardware device is faulty it must be reported to the IM&T service desk for repair or secure destruction as soon as practically possible.
- Disposal of all non-clinical IT hardware must only be carried out by IM&T and in line with Trust Policy IT09 Policy for Secure Disposal of Non- Clinical IT Equipment.
- Staff must not dispose of hardware or equipment themselves.

- All staff must ensure care is taken when printing or scanning to ensure the correct devices / accounts are selected and information is not sent to the wrong device or account.

Passwords and Pass codes

It is a criminal offence under the Computer Misuse legislation to deliberately attempt to access or modify a system to which you have no authority. UHNM monitors systems; all unauthorised attempts at accessing systems will be investigated. Passwords or pass codes that are used to gain access to systems or devices containing confidential information must be subject to the following rules:

- Must not be written down, or kept where others might find them.
- Must not be shared with any other user.
- You must not use anyone else’s password.
- Must be hard to guess and contain alpha numeric characters where appropriate.
- Must be changed at regular intervals.

Malware (Virus)

Malware, or malicious software including computer viruses, ransomware, phishing emails and SPAM, are a serious threat to UHNM. E-mail attachments and Internet sites are the most common method of infection; however it is still common for virus infection to occur from media being copied onto a PC. All UHNM employees are responsible for abiding by the following rules:

- Care must be taken when opening e-mail attachments, if unsure about the validity of an email or its attachment contact the helpdesk who will run a virus scan on the email.
- Do not remove or disable UHNM installed anti-virus software.
- All removable media, such as USB drives must be scanned before anything is copied from them
- Report symptoms that suggest to you that a PC, laptop or removable device is infected with a virus to the service desk and immediately isolate the equipment.

The deliberate or wilful introduction or circulation of Malware onto UHNM IT equipment by UHNM employees is forbidden and will result in disciplinary action in line with Trust policy.

Guidance on SPAM and unsolicited email

Email SPAM, which is also known as junk mail or unsolicited mail, involves nearly identical messages being sent to numerous recipients by email. These messages may contain disguised web links (URLs) that appear to be for familiar websites, but in fact lead to phishing websites or websites which host malware and other malicious code.

Email SPAM has increased steadily since the early 1990’s and is simply unavoidable. There are, however, a number of measures which can be (and are) taken in order to minimise the introduction of such emails into the corporate email environment.

UHNM have multiple layers of SPAM filtering in place, which prevents a large number of SPAM emails from ever reaching your inbox. These emails are manually reviewed on a daily basis to ensure that legitimate emails are not inadvertently stopped, and the appropriate action taken to ensure that the mail reaches its intended destination.

Whilst the measures detailed above prevent the delivery of a high percentage of SPAM emails from reaching your inbox, there are still a number of SPAM emails which avoid the systems we have in place, due to the constantly changing nature of the way in which this type of malicious email is created and presented to email system users.

As such, there are a number of actions which can be taken by you to help ensure that any such emails do not have an adverse impact on the corporate IT environment;

DON'T: Post your UHNM email address on any social network sites, chat rooms or webpages. Criminals use software to trawl these sites and identify email addresses, which they then harvest and turn into lists that they sell on.
DON'T: Reply to spam emails and ask to be removed. All this does is let the people sending it know your address is live and active. This will only lead you to get more spam and junk in your inbox.
DON'T: Use simple words or phrases as your email password. It means your account could easily be hacked by automated systems that try millions of different combinations of letters. Mix up your passwords and use numbers and special characters too. This will make them hard to identify.
DON'T: Pass on junk mail. What might seem a harmless joke, poem, chain letter or funny story will simply clog up the organisation's network, mail system and inboxes. Receiving so many of these types of messages are what cause people to be caught off-guard when a more sinister spam email arrives.
DON'T: Trust any email asking you for your password or other personal information. This is known as Phishing and should never ever be replied to. Report it immediately to the IM&T Department so that they can alert other users and customers, and add the content of the emails to SPAM filters, to prevent the further spread of the email.
DON'T: Believe everything you read. Spam emails will often have a false subject line to try and trick you into opening the message. It may be a tempting offer or the promise of something for nothing, but there will always be a catch. That could leave you open to all sorts of problems.
DON'T: Click on web links (URLs) contained in such emails. As detailed above, these web links may be disguised as legitimate, well known web addresses, but in fact lead to phishing websites or websites which host malware and other malicious code.
DON'T: Be fooled by the fact that the email appears to have been sent to you by someone within the UHNM mail system. If an internal user should open such an email, the mail can then reproduce itself and automatically send itself to people in the global address list, or the affected users personal address book. This automated behaviour then continues to spread the email around the Trust by going from recipient to recipient.

IM&T will never send emails asking for your password or other personal details. Banks and building societies do not send emails asking you to mail them your personal details.

If in doubt, don't open the mail, don't click on any links contained within the mail, don't forward the mail. Contact IM&T for further advice or guidance on how to proceed.

Mobile Device and Remote Working

This section relates to the security of smart phones, laptops and tablets (e.g. Apple™, Microsoft™ devices etc.) when working out of office premises. Full guidance can be found in the UHNM Operational Guidance for Remote Working and Mobile Devices Appendix C of IT07.

IM&T will supply mobile phones and other mobile devices e.g. smart phones, laptops or tablet to members of staff if required for the job role and approved by budget code holder. Employees who have been provided with a UHNM device must adhere to the following rules:

- All devices must have the screen lock functionality activated using a PIN or equivalent security setting on the device.
- Employees must not attempt to circumvent the devices' encryption or other security measures
- Employees are responsible for ensuring the safekeeping of any UHNM computing or telecommunication equipment they have been issued with.
- Any theft or loss or fault of UHNM owned equipment must be reported to Service Desk and on DATIX as soon as practically possible in order for the appropriate measures (e.g. data wipe) to be conducted.
- Use a carry case when transporting a laptop or tablet device. This will keep it dry, protect it from small knocks and keep it away from prying eyes.
- Do not leave devices or any patient information (such as medical records) in visible places e.g. a car or in a public place.
- When using the device to work remotely (e.g. on a train) ensure information on the device cannot be overlooked by non UHNM personnel and keep the device secure, in such a manner as to restrict unauthorised access to the device.

- When not in use, devices and patient information must be kept locked away and out of sight – they should not be left in cars – even locked in the boot
- Ensure that any work carried out remotely is saved on or transferred to UHNM's networked file system as soon as is as soon as practically possible.
- You must ensure that mobile devices are connected to the UHNM network at least once a month to ensure that its virus protection can be updated.
- Mobile Apps must not be used to store of transfer Trust, staff or patient information – see section 6.12.8 for more details.
- UHNM do not currently operate a Bring Your Own Device policy. Other than through approved procedures (for example the UHNM webmail) it is forbidden for employees or workers to connect non-UHNM equipment to the UHNM network or use or attempt to use such devices to access UHNM IT systems. You must not use such devices to store UHNM data.

Covert Recording

The use of recording devices has become widespread in the Trust primarily for digital dictation purposes and minute taking; these devices are easily accessible and portable making their use both convenient and time saving. However all Trust staff must be aware that there are limits to their permitted use.

The Trust prohibits the covert recording of the private words, conversations and actions of individuals without knowledge or consent, whether by way of a formal agreement or by making it expressly clear that they are recording in that area so that consent is implied.

The exception being if there is an objective reason for covert recording as part of a specific investigation or purpose, consent for which is obtained via the Trust HR Director. Any such recording is governed by the Data Protection Act and the material processed amounts to special categories of personal data; and due care is therefore taken when dealing with such information. In particular with regards to chain of custody and the integrity of recordings.

The Trust may consider the actions of those conducting covert recordings as an infringement of the human right to privacy of those being recorded.

E-Mail and Internet Acceptable Use

The Internet and e-mail systems are essential tools for employees. However, their use can expose UHNM to technical, commercial and legal risks if they are not used in accordance with the rules set out in this policy.

Breach of the rules in this section will result in disciplinary action being taken against you which could lead to your dismissal. Misuse or breach of the policy could also lead to civil or criminal actions against you or UHNM.

Permitted and Prohibited Uses

You may use the e-mail system for business use only and subject to the rules in this Policy. However, incidental and occasional personal use of e-mail is permitted, with the understanding that personal messages will be treated the same as business messages. If you do send a personal e-mail and do not wish it to be read by UHNM, this should be clearly marked as such.

Personal use of the e-mail system should never impact the normal traffic flow of business related e-mail. UHNM reserves the right to purge identifiable personal e-mail to preserve the integrity of the e-mail systems.

You should only use UHNM IT resources to access the internet if such access is required as part of your job and this should be reflected in the sites that would be reasonably expected to access. Personal use of the internet system should be limited to an hour per day at lunch time.

Information access though the secure webmail portal must not be saved to personal devices.

Personal / non Trust or non NHS.net email accounts must not be used to send any patient information.

Internet based apps must not be used to store or transmit patient data unless approved by SIRO and Information Governance.

For any queries relating to the safe sending of data contact the Information Governance team.

Offensive, Illegal and Defamatory Materials
You must not under any circumstances use the e-mail system or Internet facilities to access, download, send, receive or view any materials that will cause offence to any person by reason of:

- Any sexually explicit content;
- Any sexist or racist remarks;
- Remarks relating to a person's sexual orientation, gender reassignment, religion, disability or age.

UHNM's Equal Opportunities Policy applies to e-mail communication. You must comply with the Equal Opportunities and Dignity Policy.

You must not under any circumstances use the e-mail system or Internet to access, download, send, receive or view any materials that you have reason to suspect are illegal. Please refer to the second part of this Policy entitled "A Guide to the Legal Issues" for guidance on what materials may be illegal.

Please remember that it may be illegal to copy many materials appearing on the Internet including computer programs, music, text and video clips. If it is not clear that you have permission to copy materials off the Internet, please do not do so.

You must not send or circulate any materials on the Internet or by e-mail that contain any negative remarks about other persons or organisations. Any use of the e-mail system or Internet access for any of these prohibited purposes will be treated as a serious disciplinary matter which may lead to dismissal of the employee concerned.

Whilst UHNM takes all reasonable precautions to prevent access to internet sites that may relate to or contain inappropriate content, for example - adult and sexually explicit material, alcohol and tobacco, criminal activity, gambling, games, intolerance and hate, illegal drugs and violence - it cannot guarantee this protection for all internet sites all of the time. If you unintentionally access such sites (including pop-ups) you should immediately isolate the equipment you are using and immediately report the incident to the IM&T Service Desk, your Line Manager and raise an incident on DATIX. You must not intentionally access or attempt to access inappropriate content from UHNM IT equipment.

Monitoring
UHNM reserves the right to monitor and inspect any e-mails sent by you using the e-mail system, including personal messages, at any time without notice. Such monitoring is automated and intended to ensure that this Policy is being adhered to, is effective, and that UHNM and its employees are acting lawfully.

You should therefore have no expectation of privacy when using the e-mail system and other methods of communication should be used for any messages you wish to keep private.

All connections to the Internet are monitored and recorded in log files. Such monitoring of the Internet usage is solely to ensure that this policy is being adhered to and that UHNM and its employees are acting lawfully. These files record information of which site has been accessed and by whom. They are checked automatically on a regular basis.

Confidentiality and Special Categories of Personal Data
Please remember that e-mails are not necessarily a secure way of sending information. If you want to use e-mail to send any information which is highly confidential (i.e. it could cause the UHNM loss or embarrassment if it were publicly disclosed or fell into the hands of a competitor), then you must follow these rules:

- Such information must be encrypted. Please contact the Help Desk who will advise you on how to encrypt information;
- Obtain authorisation from your manager where this is a new requirement or is not an agreed part of your job role.

The following categories of information will be treated as highly confidential:

- Information about patients;
- Personnel records;
- All information received under a duty of professional confidence from a patient, carer, colleague or another member of staff.

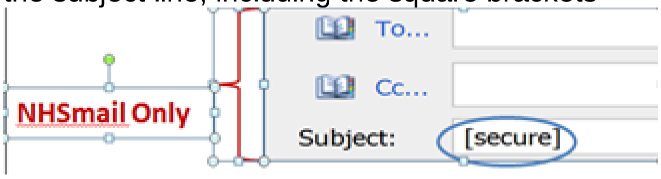
All e-mail must contain UHNM's standard e-mail notice containing the confidentiality notice and disclaimer. That notice is generated automatically by the e-mail system and it should not be removed in any circumstances.

Please also be aware that e-mail messages, like paper based documents, may be subject to disclosure under the Data Protection Act, the Freedom of Information Act and can be required to be produced in legal proceedings. If you would not like an e-mail to be produced in court, viewed by a patient or carer or made public, please refrain from using e-mail.

E-mailing Patient or Special Categories of Personal Data
Do not send unencrypted patient data outside the local health economy and the COIN. North Staffs COIN (Community of Interested Networks) is a private local Health Economy network specifically developed for the use of the local health economy including;

- University Hospitals of North Midlands
- North Staffs Combined Healthcare (NSCHT)
- Midlands Partnership Foundation Trust (MPFT)

Secure email sending is as follows:

@uhnm.nhs.uk		@staffordshirecss.nhs.uk @SSOTP.nhs.uk @stoke.nhs.uk @northstaffs.nhs.uk @mpft.nhs.uk
@uhnm.nhs.uk		@uhnm.nhs.uk
@nhs.net		@nhs.net
@nhs.net		@mcht@nhs.uk
@nhs.net		@anyother ONLY if you put [secure] as the first word in the subject line, including the square brackets  Subject: [secure]

Housekeeping
The following rules will help systems to work more efficiently. Please adhere to them at all times.

- All important e-mail messages must be filed or stored in your secure network drive.
- Where possible, obtain confirmation from the recipient that an important e-mail has been received.

- If you receive a wrongly delivered message you should inform the sender and delete it, if the e-mail message contains confidential information you must not make use of that information and must not disclose it.
- Messages must be deleted on a regular basis or stored in a suitable electronic file.
- E-mails to All-user must be avoided if possible as they cause system congestion.
- Do not subscribe to e-mail services which will result in e-mails being sent automatically to you unless these are useful for your job.
- Do not send out trivial or personal e-mail messages. These lead to congestion of the e-mail system and reduce its efficiency.
- You must not delete or copy emails without the agreement of your manager;
  - if you change role or department or
  - if you leave UHNM employment,

Remember. Treat e-mail in the same way you would treat a letter or fax. Do not e-mail a message that you would not want read out in court.

Social Media Use
Social Media' or 'networking' sites refers, but is not limited to the following online resources:

- Personal blogs
- LinkedIn
- Twitter
- Facebook
- Instagram
- Personal Web sites
- Community forums – e.g. developer websites, hobby sites, sports forums, specialist interest groups etc.
- Internet chat rooms
- Online encyclopaedias – such as Wikipedia

Posting on social networking sites by employees, whether using the UHNM s' property and systems or personal computer systems, is subject to the terms and restrictions set out in this policy. You are reminded that your duty of confidentiality to UHNM also applies to social networking. As such, employees are prohibited from revealing personal or special categories of personal data about patients, carers or UHNM employees, any UHNM confidential or proprietary information or trade secrets.

Employees shall not engage, even in their own time, in any social networking;

- that may harm or tarnish the image, reputation and/or goodwill of UHNM and/or any of its patients, employees, workers, suppliers or clients
- which is detrimental to the UHNM 's interests
- that involves bullying or harassment of, or making disparaging or derogatory comments about any of the UHNM's patients, employees, workers, suppliers or clients
- that involves posting or misusing patients or other employees' personal data or information, where that information has been accessed from the UHNM without the consent of the patient or other employee.

UHNM reserves the right to routinely monitor all employees for the purpose of ensuring that UHNM rules are being complied with, investigating wrongful acts, or complying with any legal obligation. You should have no expectation of privacy when using UHNM's systems or property.

Any breach of this policy will to result in disciplinary action being taken. A serious breach of this policy may be considered to amount to gross misconduct warranting dismissal. The following are non-exhaustive examples of the type of behaviour which may be regarded as gross misconduct:

- Posting Company, client or supplier confidential information online

- Any form of harassment, bullying or discrimination against any of the UHNM ’s employees, workers, suppliers or clients
- Making derogatory, damaging or offensive comments or statements about any of the UHNM ’s employees, workers, suppliers, clients or competitors
- Online posting of personal data or information which you have obtained from UHNM about a patient or carer, without their consent
- Online posting of personal data or information which you have obtained from UHNM about another employee or worker, without their consent
- Any activity that may bring UHNM into disrepute or damage or lower the UHNM ’s reputation

For further guidance on posting material on social media, please contact the Communications Department.

For further guidance on this policy please contact either your manager, or the Information Security Manager.

Internet based apps.
Internet based apps must not be used to store or transmit patient data unless they have been approved for use by the Trust SIRO and Information Governance, this includes but is not limited to apps such as WhatsApp, personal Skype accounts, messenger or Hospify.

A Guide to the Legal Issues Relating to Use of E-mail and the Internet
This section of the Policy is intended to give employees guidance on the most important legal issues which may arise from their use of the e-mail system and Internet access.

It is very important that you read this section to understand those issues as this will help you, and UHNM, to avoid problems.

These are not just theoretical issues. If the law is broken then this will lead to one or more of the following consequences:

- Civil and/or criminal liability for yourself and UHNM;
- Disciplinary action against you which may include your dismissal.

Bullying and Harassment
UHNM requires all employees to be treated with dignity at work, free from harassment and bullying of any kind. Harassment can take the form of general bullying, or be on the grounds of sex, race, disability, sexual orientation, age, religion. Harassment could include sending sexist or racist jokes, making sexual propositions or general abuse by e-mail. You must not send any messages containing such material.

Bullying and harassment of any kind will be treated as a serious disciplinary matter which may lead to dismissal.
If you are subjected to or know about any harassment or bullying, whether it comes from inside or outside the organisation you are encouraged to contact your line manager immediately.

Breach of Copyright
Materials that you encounter on the Internet or receive by e-mail are likely to be protected by copyright. This will apply to written materials, software, music recordings, graphics and artwork and video clips. Only the owner of the copyright, or other persons who have the owner’s consent, can copy those materials or distribute them.

If you copy, amend or distribute any such materials without the copyright owner’s consent, then you may be sued for damages. UHNM may also be liable and, in some circumstances, criminal liability can arise for both you and UHNM.

Be particularly careful not to copy text or to download software or music unless you are sure you have permission to do so. Always check the materials in question to see if they contain any written prohibitions or permissions before you copy or download them.
Never download any software, music recordings or other materials that you know to be fakes or "pirate copies".

Unwanted Contracts
An exchange of e-mail messages can lead to a contract being formed between you or UHNM, and with the intention that legal obligations should arise and some payment or other consideration being made for the performance of those obligations. Breach of contract can expose UHNM to a claim for damages.

Contracting by e-mail is subject to the same requirements as any other form of contract. You must adhere to UHNM's established policies and procedures about purchasing and contracting.

Never commit UHNM to any obligations by e-mail without ensuring that you have the authority to do so. If you have any concerns that what you are doing will form a contract, contact your manager and the Supplies and Procurement Department.

Mark all e-mails relating to contractual negotiations "Subject to Contract". You should also ensure that any person with whom you wish to enter into a contract is adequately identified. All e-mail contracts will require the use of digital signature technology to ensure that their identity is affirmed and to ensure the integrity of content of the contract. Please contact the Help Desk for guidance on the use of digital signatures.

Any contract entered into via e-mail must contain the following statement:

"Any contract formed by this e-mail will be governed and construed in accordance with the laws of England and the parties submit to the non-exclusive jurisdiction of the English courts". Beware of any attempt by the party with whom you are dealing to incorporate its own terms and conditions into a contract.

Defamation
If you send an e-mail (NB: even an internal e-mail), or post any information on the Internet, which contains any remarks which may adversely affect the reputation of another organisation or person, you will be exposing both yourself and UHNM to the risk of legal action for defamation.

This is a real risk. Organisations have been sued for the defamatory contents of e-mails sent by employees and have been required to pay out considerable sums as a result.

Obscene Materials
You must not under any circumstances use the e-mail system or Internet to access, display, circulate or transmit any material with a sexual content. This may constitute a criminal offence and both you personally and UHNM could be liable.

Sexual harassment will be treated as a serious disciplinary matter which may lead to dismissal.

Data Protection Act
Information about a patient and/or an employee (the Data Subject) is confidential and should not be disclosed to anyone who does not have a right to know it.

You must not disclose personal data to other employees unless it is needed for work purposes. Do not leave personal data or files unguarded in areas where the access cannot be controlled. Customer files must not be taken home unless in rare circumstances your Manager authorises it. All computer produced output and manual records must be securely disposed of.

We must have written authority from the Data Subject before disclosing information to a third party, e.g. banks, solicitors. Any other requests for information, either in writing or on the telephone, e.g. from the

Police, Inland Revenue or any other body must be referred to the Trusts Information Governance Manager in the first instance.

Under the Data Protection Act a patient may have a right of access to their personal data held manually or on computer. They also have the right to have any information held by us to be corrected, blocked or have the information amended if it is regarded as wrong or incorrect information. They must however, put this request in writing by completing an access to Health Records form or e-mailing ministries.office@uhnm.nhs.uk

As an employee also have a right to request HR information about you held both manually and on computer by UHNM. This request must be made in writing and sent to the Human Resources Department. You also have the right to request that incorrect information is rectified, block or amended if regarded as incorrect.

Breach of the Data Protection Act is a criminal offence.

For further information see IG07 Information and Governance Management Framework and Policy and IT08 Internet and E-mail policy

5. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

It is a national requirement that all NHS staff undertakes annual Information Governance training, information governance training is included in the Trust's mandatory training programme. For queries regarding Information Governance training contact the Information Governance Department.

Prior to operating any hospital clinical information system (EPR, RIS, Pathology etc.) all users are required to undertake system training according to the access level required for the job role undertaken. Information Security training will be included in all IM&T managed training courses - user login and password will not be issued prior to the users attending this course.

Divisions who manage their own independent Divisional information systems such as but not exclusively, CRIS, Pathology, Renal and Finance, must ensure there is a nominated lead (Information Asset Owner) who is responsible for ensuring the appropriative training is provided to staff who operate the system. This information must be recorded as it may be required to be evidenced for audit purposes.

This training should be held in the staff personal record, ideally within ESR.

6. MONITORING AND REVIEW ARRANGEMENTS

6.1 Monitoring Arrangements

IM&T will undertake routine monitoring of the Trusts IT systems, this will use a variety of monitoring tools both automated and manual, this includes but is not limited to;

- Web Filtering Services to record and monitor web sites visited (live time)
- Mail content filtering to block certain file types (live time)
- Antivirus software to monitor for virus's and malware (live time)
- Ad hoc Audits of access to, and permissions to Trust Systems
- Ad hoc audits of file types stored on Trust network storage
- Monthly audits of unused domain accounts
- Network monitoring tools (live time)

Routine monitoring will not include opening of personal e-mails or files.

All monitoring and investigation work will be carried out in accordance with G09.

Where the results from routing monitoring show undesirable activity this will be reported to the Head of Service Delivery and Information Security Manager in the first instance who will investigate in conjunction with the Trusts Information Governance Manager and Data Protection Officer as appropriate, such activity will result in disciplinary and / or legal action.

Non routine monitoring may also take place in the case of criminal or disciplinary investigations in line with Trust policies under the advice of the Human Resources department.

Breaches or suspected breaches of this policy can be reported directly to IM&T by all members of staff, additionally breached can be reported confidentially via the HR30 Whistle Blowing Policy

Compliance with Information Governance Training and induction training will be monitored on an annual basis in line with the Trusts Information Governance Toolkit requirements.

Sign off of the Standards for Personal Information Security and Acceptable Use will be required prior to new users gaining access to UHNM IM&T resources. Users may also be asked to re-sign should significant changes to these standards be made.

6.2 Review

This policy is managed and controlled by the Information Security Manager and shall be reviewed by the Information Governance Steering Group as part of the processes within the organisations Information Security Management System.

This policy will be reviewed within one year of its first acceptance date and then every three years or more frequently if there are changes in related legislation or other standards, or if significant risk and / or issues are identified. This policy may also be subject to internal and external audit.

In addition the contents of this policy will be reviewed annually by the Information Governance Steering Group against the Information Governance Toolkit Requirements as part of the Trust self-assessment process.

7. REFERENCES

Data Protection Act	www.ico.org.uk
Regulation of Investigatory Powers Act 2000	www.legislation.gov.uk/ukpga/2000/23/contents
Human Rights Act 1998	www.legislation.gov.uk/ukpga/1998/42/contents
Equality Act 2010	www.gov.uk/guidance/equality-act-2010-guidance
Civil Contingencies Act 2004	www.legislation.gov.uk/ukpga/2004/36/contents www.england.nhs.uk/ourwork/eprr/
NHS Information Governance Framework	www.systems.hscic.gov.uk/infogov
ISO/IEC: 27001 Information Security Management Standard	www.iso.org
CESG: the Information Security Arm of GCHQ	www.cesg.gov.uk

APPENDIX A: STANDARDS FOR PERSONAL INFORMATION SECURITY AND ACCEPTABLE USE ACCEPTANCE SIGN OFF FOR ALL USERS

Standards for Personal Information Security and Acceptable Use – All Users Acceptance sign off

By signing this I acknowledge that I understand my personal responsibility to take all reasonable measures to prevent a breach of Information Security as a result of my actions, and further, that a breach of the rules in this Policy will result in disciplinary action being taken against me which could lead to my dismissal and could also lead to civil or criminal actions against me or UHNM.

I understand that if I have responsibilities as a manager I will also need to sign off Appendix B, and if I required enhanced access rights for my job I will need to sign of Appendix C.

Your Name: ____

Your Signature: ____

Date: _____________________

Your Managers Signature: ____

Date: _____________________

(Please sign two copies of this statement, return one copy to your manager and keep the other for your records.):

APPENDIX B: STANDARDS FOR PERSONAL INFORMATION SECURITY AND ACCEPTABLE USE – ADDITIONAL MANAGERS RESPONSIBILITIES

Information security is a key responsibility of all managers and is referenced in all staff contracts and job descriptions. This agreement aims to ensure that you are aware of your information security responsibilities. You are reminded that you are personally responsible for ensuring that no breaches of information security result from your actions. Failure by you to apply controls in handling personal, patient or special categories of personal data that does lead to a breach will amount to gross misconduct and result in disciplinary and/or legal action.

This agreement based on the Trust policies:

IT07 – Trust Policy form Information Security Management and
IT08 – E-Mail and Internet Policy

Further supporting information may be found in the following documents:

- IG07 Information and Governance Management Framework and Policy
- RM01 Risk Management Policy and Strategy
- RM07 Management of untoward Incidents including Serious Untoward Incidents
- RE01 Multidisciplinary Health Records Policy
- RE02 Clinical Photographic and Video Policy
- IG08 Freedom of Information Act Policy
- G11 Corporate Records Management Policy
- G09 Trust Policy for the Management, Protection and Disclosure of Employment Related Information
- HR53 Statutory and Mandatory Training Policy
- HR01 Disciplinary Policy and Procedure
- HR17 Trust Policy for Induction Training
- ICT04 Operational Guidance for Accessing Account of Absence Staff
- ICT05 Operational Guidance for Use of Generic E-Mail Accounts
- ICT06 Operational Guidance for Guidance on Sending Personal Identifiable / Sensitive Information By E-Mail

This Agreement outlines the Trusts information security expectations for managers whose staff have access to electronic information systems provided by the Trust or its health and social care partners for the:

- Management and treatment of patients and carers,
- The administration of the Trust

Separate specific guidance is provided for all staff and users with enhanced security privileges- for example System Managers.

All UHNM Managers are responsible for abiding by the following rules:

General responsibilities:
Ensure that all my staff are aware of:

- Their obligations to maintain patient and staff confidentiality
- Corporate and local Information Security policies and procedures
- Their personal responsibilities for Information Security
- That personal files and folders must not be held on Trust computers or network servers
- How to access advice and guidance on Information Security

All UHNM Managers are responsible for abiding by the following rules:

- How to report Information Security incidents using the Trusts Adverse Incident Reporting Process
- The legal and disciplinary consequences of not complying with their Information Security obligations
- That gaining or granting unauthorised access to any of the Trusts IT systems is a disciplinary matter

Ensure that my Managers:

- Are aware of their responsibility to make their staff aware of acceptable standards of information security.

Notify IM&T and relevant system managers of any changes to my staff or their circumstances that may affect access to systems, including:

- Starters and leavers
- Change of job title
- Change of job role
- Change of work location

Investigate and where appropriate, initiate disciplinary proceedings, where I have reason to believe a member of my staff is in breach of Trust Information Security Policies and Procedures.

Notify IM&T of any unused IT equipment.

Verify that all contractors undertaking work for or on behalf of the Trust have signed confidentiality (non-disclosure) undertakings.

Ensure that there are local procedures for ensuring the physical security of IT equipment and information within areas I have a responsibility for – examples include, locking windows and doors, clear desk policies in insecure areas.

Management of systems:
Determine and authorise the levels of access individuals have to systems based on their job role.

Support audits of system access.

Implement procedures to minimise the Trusts exposure to fraud, theft or disruption of services.

Ensure that process documentation for critical job functions is maintained.

Ensure that at least 2 members of staff have the expertise and training to manage or administer any locally managed systems that I have a responsibility for.

Information Security education and training:
Ensure that all my staff receive appropriate systems training when starting at the Trust, when there is a change job function that affects how they use systems, system changes and receive refresher training on a regular basis.

Ensure all my staff receive appropriate levels of education, training and development in all aspects of information security.

Ensure that my local induction programme includes Information Security as mandated by

All UHNM Managers are responsible for abiding by the following rules:
HR17- Trust Policy for Induction Training.

Ensure that up to date training records are maintained in staff records to prove attendance and competency.

Leavers:
Review with leavers (either leaving the Trust or when changing roles) any of my member of staffs files and e-mails to decide if they need to be retained beyond the standard 90 retention for leaver's data.

Identify any generic or departmental accounts held in the name of the user and ensure the IM&T Department know who they are to be transferred to at least 1 week in advance of the leaving date.

If business files from the member of staffs accounts are to be retained, advise ICT of who will be managing this process and by when the files will have been transferred to another account.

Notify the IM&T Department once files have been transferred.

Ensure that the member of staff is aware that they are not to delete files without prior agreement from me.

Ensure that any equipment issued to a member of my staff (such as laptops, USB sticks and other removable storage devices) are promptly returned to ICT when a member of my staff leaves the employment of the Trust.

Be aware that files remaining in the member of staffs accounts will be held for 90 days prior to deletion.

Long term absence:
Ensure that I notify IM&T of any member of staff on long term absence and who will not be accessing their account for over 90 days.

Review if there is a need to access the accounts of members of my staff who are or are likely to be away from duty for an extended period, identify who will be given access and notify the member of staff that their accounts will be accessed.

If there are risk assessed operational needs to access an absent member of my staff's accounts, then I will follow the processes in ICT04 – Operational Guidance for Accessing Account of Absence Staff.

Remote working:
Identify and authorise access for members of my staff whose role requires them to access the Trusts network (files, e-mails, systems) remotely.

Ensure that a copy of this requirement and authorisation is held within the member of staffs Personnel File.

Ensure that staff who require remote access are aware of their additional responsibilities in relation to Information Security as per the Trusts Remote Working and Mobile Devices guidance in appendix C of IT07.

Periodically review remote and home working agreements to ensure that they are being maintained or if they need to be revoked.

All UHNM Managers are responsible for abiding by the following rules:
Notify IM&T immediately if a member of staff with remote access has their employment terminated.

Information Security - Use of UHNM Trust ICT resources - Managers Agreement –

Acceptance sign off

By signing this I acknowledge that I understand my personal responsibility to take all reasonable measures to prevent a breach of Information Security as a result of my actions, the actions of staff reporting to me and further, that a breach of the rules in this Policy will result in disciplinary action being taken against me which could lead to my dismissal and could also lead to civil or criminal actions against me or UHNM.

Your Name: ____

Your Signature: ____

Date: _____________________

Your Managers Signature: ____

Date: _____________________

(Please sign two copies of this statement, return one copy to your manager and keep the other for your records.)

APPENDIX C: STANDARDS FOR APPROPRIATE USE OF ENHANCED ACCESS RIGHTS TO IT SYSTEMS

Audience

These standards are intended for use by all Trust Information Asset Administrators, Systems and File Administrators, and staff within the IM&T Department.

Trust Information Asset Owners may wish to include these Guidelines within their System Level Security Policies (SLSPs).

Introduction

Enhanced or Privileged access levels are defined as levels of access above that of a normal user, this can include super user, power users, local admin, system administrator or simply access to records which would not normally form part of your role – e.g. the ability to view patient records whilst you are not clinically involved in that patients care.

Normal end users are protected, by inbuilt system controls, from carrying out actions that would endanger the availability, integrity or confidentiality of data held within Trust systems. Those with enhanced rights do not have these same protections in place, it is therefore vital that in order to protect both the information and this group of users, appropriate access is clearly defined, recorded, and monitored.

The importance of having robust privileged access controls has never been more important with hackers targeting privileged accounts, often finding credentials in unprotected files, such as spread sheets.

As you have enhanced access rights you are being asked to sign this declaration to indicate you understand and agree to the conditions of its use and the key principles that support:

- Appropriate and inappropriate use of enhanced access
- Governance of usernames and passwords
- Accessing special categories of personal data, Staff or Corporate Records

Appropriate use of enhanced access

- The use of Enhanced Access should always be consistent with an individual’s role, or job responsibilities as defined by management - if such access is not reflected in your job description you should ensure that the requirement is recorded by your line manager in your personnel file.
- When your role or job responsibilities change, any levels of enhanced access must be appropriately updated or removed.
- In situations where it is unclear whether a particular action is appropriate and/or within the scope of your current job responsibilities, the situation should be clarified and the outcome agreed with management before proceeding.
- All users, especially those who have, or manage those who have enhanced rights, have a responsibility to question the legitimacy of their access - continuing with old processes because ‘we’ve always done it that way’ or ‘it’s more convenient’ are not suitable defences for inappropriate access.

Inappropriate use of Enhanced access right

Whilst not an exclusive list, the following actions are viewed by the Trust as being an abuse of enhanced access rights:

- Using enhanced rights to circumvent user access controls or any other security or computer controls in place.
- Circumventing formal account creation and deactivation procedures
- Circumventing formal change request procedures
- Circumventing any other Trust procedures that are formally approved by management or ratified Trust wide
- Accessing Non-public Information that is outside the scope of specific job responsibilities

- Exposing or otherwise disclosing Non-public Information to unauthorised persons
- Using access to satisfy personal curiosity this could be about your own record, friend, neighbour, co-worker or even a person of public interest.

Usernames and Passwords

In order for certain actions to be carried out such as development, user administration, backup and recovery and testing, it may be necessary for an individual to have multiple logins with differing levels of access. Where this is the case the following rules apply;

- Do not share user names and passwords
- Do not share logged in sessions
- On set up any secondary, accounts must clearly be identified with you and the reason for enhanced access explained and documented.
- Use the login with the lowest level of access whenever possible and do not default to using enhanced accounts as a usual occurrence, i.e. it is unnecessary to use Dr's access to simply view a ward listing, or use a login with domain privileges in to access your e-mails.
- Do not use default accounts with privileged access, such as SysAdmin, rather use secondary accounts with similar permissions
- Ensure that enhanced accounts utilise complex passwords and that passwords are changed regularly.

Accessing Patient Records

Under normal circumstances only test patients should be used – available accounts for each systems are as follows;

- A111
- B111
- C111
- D111
- E111
- F111
- G111
- A222
- B222
- C222
- D222
- E222
- F222
- G222
- H333
- K65000
- P63050

Under certain circumstances there will be a requirement to access live patient data, i.e. to resolve an issue with a particular record. Where this is required this should only be carried out with senior management approval, and access should be recorded including the following details;

- Patient NHS number
- Patient unit Number
- The name of the staff member accessing the record
- Reason for access / Actions taken
- Data and Time
- Authorising Manager / notified manager if accessed in error

This should be recorded in the call logging system against the request where possible, or in the users personal file along with an e-mail communication authorising the request. The same details should be recorded if a live patient record is accessed in error, along with raising the error as an incident on the Trusts adverse incident reporting system (DATIX). This recording protects the individual staff members from recrimination should the legitimacy of any access be queried.

Accessing Staff Records

Under certain circumstances there will be a requirement to access live personnel data, i.e. to resolve an issue with a particular record. Where this is required this should only be carried out with senior management approval, and access should be recorded including the following details;

- Staff Members Trust identifier (e.g. Assignment number)

- The name of the staff member accessing the record
- Reason for access / Actions taken
- Data and Time
- Authorising Manager / notified manager if accessed in error

This should be recorded in the user's personal file along with a copy of an e-mail communication authorising the requirement. The same details should be recorded if a live record is accessed in error, along with raising the error as an incident on the Trusts adverse incident reporting system (DATIX). This recording protects the individual staff members from recrimination should the legitimacy of any access be queried.

Testing
System testing, either for new functionality or new systems that use special categories of personal data, should only be carried out with test data, or with anonymised personal data. Where migrated records are used as part of acceptance testing, the use of patient or special categories of personal data details must be included in the test script. Where live identifiable data is used for testing a record of the specific details and the authorisation should be kept securely, ideally in a locked location or pass-worded file for audit purposes.

Sharing records
Person identifiable and/or special categories of personal data must not be sent by Trust e-mail account unless the sender complies with ICT06 – Operational Guidance on Sending Personal Identifiable/special categories of personal data Information by E-Mail.

Person identifiable and/or special categories of personal data must not be shared with 3rd parties unless there is a current data sharing agreement in place covering the use for which the information is being provided. For example a sharing agreement which states a 3rd party may view patient data whilst resolving issues through a secure remote access function, would not entitle them to a copy of the data for testing purposes.

All end user access is open to audit, and as Patients are entitled to request who has accessed their records this could be disclosed through any disciplinary or operational monitoring process.

Standards for appropriate use of enhanced access rights to IT systems

Acceptance sign off
By signing this I acknowledge that I understand my personal responsibility to take all reasonable measures to prevent a breach of Information Security as a result of my actions, the actions of staff reporting to me and further, that a breach of the rules in this Policy will result in disciplinary action being taken against me which could lead to my dismissal and could also lead to civil or criminal actions against me or UHNM.

I understand that the completion of this form will not automatically guarantee such access and that this will need to be requested from IM&T evidencing this sign off.

Your Name: ____

Your Signature: ____

Date: ____________________

Your Managers Signature: ____

Date: ____________________

(Please sign two copies of this statement, return one copy to your manager and keep the other for your records.)