University Hospitals of Leicester NHS
NHS Trust

INFORMATION SECURITY POLICY

Approved By:	Trust Board
Date of Original Approval:	9 October 2003
Trust Reference:	**B40/2024 (Previously A10/2003 agreed at 11/04/24 Trust Board)**
Version:	5
Supersedes:	4 – June 2020 PGC
Trust Lead:	Saiful Choudhury – Head of Privacy
Board Director Lead:	Andrew Furlong – Medical Director
Date of Latest Approval	11 January 2024 – Trust Board
Next Review Date:	**January 2027**

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

2023 review - EIMT replaced with The Trust Leadership Team.

Policy links updated

Roles section updated

Clarification of responsibilities (Section 4.5)

Examples of assessments given (Section 5.3)

Clarification on physical and security of information (sections 5.25 and 5.25.1

References to BYOD and Agile working updated

KEY WORDS

1 INTRODUCTION AND OVERVIEW

This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures that applies to all Trust business and covers the information, information systems, networks, physical environment, employees and contractors who support those business functions including where these facilities are shared with or owned by external partners**.** The policy will be complied with in conjunction with other approved Trust policies and with other legal obligations of UHL.

2 POLICY SCOPE

21 The purpose of this policy is to ensure that information processing systems, and electronic or paper based information, are protected from events that may jeopardise staff and patients' rights to confidentiality, other healthcare activities or, the business objectives of UHL.

The rules, measures and procedures described herein determine the protection of the Trust's assets by ensuring that:-

- Information systems are properly assessed for security.
- Availability is ensured (information is delivered to the right person, when needed and adhering to the organisation's business objectives).
- Integrity is maintained (all system assets are operating correctly according to specification, protected from unauthorised or accidental modification, and ensuring accuracy and completeness of the organisation's assets).
- Confidentiality is preserved (assets are protected against unauthorised disclosure).
- Accountability is enforced (staff are made aware of and held to account for their roles and responsibilities in regard to information security).
- Breaches of information security are detected and resolved.

This Policy only applies to UHL devices and any personal devices that have been approved via the Bring Your Own Device (BYOD) process. It will then be refered to as a UHL device within the rest of this policy. Please see Mobile Device Management Policy in Section 9.

3 DEFINITIONS AND ABBREVIATIONS

3.1 **Electronic media** (eg. Floppy disks, USB or Pen drive, CDs and DVDs, External hard drives, Cameras, PDAs, Mobile telephones and Dictaphone tapes.

3.2 **Virtual Private Network (VPN)** allows users to connect to the trust network and resources securely over the public network via trust devices (internet)

3.3 "**Bring your own device" (BYOD**) refers to the use of personal mobile devices to access UHL administrative and clinical applications through the secure trust wifi network internally or over their mobile internet if externally accessing. Further guidance can be obtained from the Head of Privacy on 0116 2586053

4 ROLES

4.1 **Senior Information Risk Officer and Executive Lead**: The Senior Information Risk Officer (SIRO) has executive board level responsibilities and reviews the Trust's IG processes and provides written advice to the Chief Executive on the content of the Trust's Annual Governance Statement in regard to information risk. UHL SIRO is the Chief Information Officer.

The key responsibilities of the SIRO are:

- To review the IG strategy, implementing the policy within the existing Framework including the Information Security Management System (ISMS);

- To assess the risk assessment process for information governance, including review of the annual information risk assessment to support and inform the Annual Governance Statement and compliance submissions including IG & DSPT;
- To review and agree action/s in respect of identified IG work programme and associated information risks.

4.2 **Caldicott Guardian:** The Trust Caldicott Guardian has Executive board level responsibilities for the Trust's Caldicott Function and enables a direct reporting line to the Trust Board and the appropriate governance committee. The Caldicott Guardian's main responsibility is to be responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing. This links directly to IG executive lead and will require the IG Lead to liaise directly to discuss information sharing issues.

UHL Caldicott Guardian is the Medical Director.

The additional responsibilities of the Caldicott Guardian are;

- ensuring that the Trust processes satisfy the highest practical standards for handling patient information in line with Caldicott Principles for information sharing;
- advising on policy issues to update standards with regard to patient data;
- Advocating policy requirements at Executive board level to protect patient interests.

4.3 **Information Governance Steering Group :** The Information Steering Group is responsible on behalf of the Chief Executive for all matters relating to this policy including;

- developing, implementing and maintaining a IG strategy and associated standards, an implementation strategy including an annual work programme to provide assurance to the Trust that effective arrangements are in place;
- Reporting to the SIRO on annual basis to clarify performance and risks issues identified during audit and training cycles for executive level consideration.
- To determine staff have a legitimate business need for a Trust issued device or BYOD connection as well as ensuring that the mobile device is being used as a business tool.

4.4 **Trust IG Lead:** The nominated IG Lead is the Head of Privacy within the IMT department. The Trust's Head of Privacy has responsibility for managing the overall co-ordination, publicising and monitoring of the Trust IG Framework. The Trust's IG Lead has specific responsibility for;

- the development of the IG strategy and policy, procedure and guidance;
- leading training and audit strategies to raise IG standards and services;

- producing IG performance monitoring reports and submitting annual compliance assessments as required;
- Producing DSPT central returns on behalf of the Trust.
- Ensuring compliance with Legal requirements

4.5 **Employees & staff working on behalf of the Trust:** All Trust employees, whether permanent, temporary or contracted, and students and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. This policy requires all staff to understand the need;

- To comply with all information standards;
- To hold information securely and confidentially;
- To obtain information fairly and efficiently;
- To record information accurately and reliably;
- To share information appropriately and lawfully

The Additional Responsibilities are:

4.5.1 **Line Managers** are responsible for ensuring that their permanent or temporary staff and contractors are aware of:-

- The information security policies which are applicable in their area;
- Their personal responsibility for information security;
- How to access advice on information security matters.

4.5.2 **Staff members** all have a responsibility for the security of information in electronic or manual systems. This includes:

- Not sharing logins, passwords or smartcards;
- Ensuring that personal data in electronic format stored on portable media is encrypted.

Members of staff who originate **new or revised flows of personal data** within and outside of the Trust are responsible for ensuring that information flow mapping is carried out, the information security risks of the data transfer are assessed (seeking advice from IM&T where appropriate).

5. POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS

5.1 Information will be protected against access by individuals who do not have a justified and approved business need (i.e. unauthorised access) by the use of appropriate logical access controls and physical access controls.

5.2 All computers will operate up to date anti-virus software.

5.3 All UHL capital projects incorporating requirements for IT services or the transfer of data outside of the Trust will include appropriate information security assessment. These assessments could be DPIA (Data Protection Imapct Assessment), DSA (Data Sharing Agreement) and DTAC (Digital Technical Assessment Criteria) amongst others. You should contact the Privacy Departmetn for help with this.

5.4 IM&T will build resilience into services in accordance with business need. Disaster recovery plans will be produced, maintained and tested by IM&T.

5.5 All breaches of information security, actual or suspected, will be reported to, and investigated by IM&T who will document the incident and where necessary will report the findings of these investigations to the IM&T Steering Group. This is reported via Datix.

5.6 The physical security afforded to information will be commensurate with the operational requirements of the Trust, the value of the equipment and the nature of the information held on and/or processed by it.

5.7 All equipment should be clearly marked as being the property of the University Hospitals of Leicester NHS Trust.

5.8 Any minor changes to the use or structure of 'live' systems will be subject to a formal change control procedure held by IM&T. Fundamental changes to 'live' systems together with the introduction of new systems will be subject to the full Project Management process.

5.9 ALL UHL Laptops must be encrypted to NHS encryption standards.

5.10. Software licensing applies to all UHL devices, only licensed software provided for that purpose must be used

5.11 At the termination of employment, employees must return all data processing equipment, tokens, smartcards & data stored on devices supplied for that purpose.

5.12 IM&T will maintain an asset register of key Trust IT assets; this will include all IT hardware and software.

5.13 UHL will use Risk Management procedures to estimate threat probability, including information security risks to IT systems; their vulnerability to damage, and impact of any damage caused. Such assessments are the responsibility of the System Owners (i.e. those within the Directorates/Departments who are responsible for the day to day operation of the specific system). Measures will be taken to ensure that each system is secured to an appropriate and cost effective level and that data protection principles are implemented.

5.14 Management of computers and networks shall be controlled through standard documented procedures that have been authorised by IM&T.

5.15 UHL will adopt national standards for the security classification of information.

5.16 The movement of unencrypted personal data in electronic format on portable media e.g. CDs, memory sticks is strictly prohibited. See 5.25.4 Using Removable Media.

5.17 An audit trail of system access and data use by staff will be maintained by IM&T. Access of the audit trail for investigatory purposes will be carried out in accordance with documented HR procedures which conform to the Regulation of Investigatory Powers Act (2000) and the Human Rights Act (1998).

5.18 All computers and electronic media must be disposed of through IM&T. This includes computer disks (which contain personal data) from medical equipment. See 5.27

5.19 External hard drives are only to be used with the approval of the Technical Security Specialist. If approval is given, the device must be encrypted.

5.20 The information security arrangements for equipment and software must not be circumvented.

5.21 Only PDA's and smart phones provided by UHL must be connected to UHL equipment.

5.22 Users should adopt a clear desk and clear screen policy for confidential or personal data to reduce the risks of unauthorised access, or accidental damage to or loss of sensitive or confidential information.

5.23 Companies like Microsoft and Google make software and data storage available to users through web browsers (e.g. Google Docs, Windows Sky Drive). Users are forbidden to use web hosted applications and data storage as the confidentiality, security and integrity of the data (which is held external to UHL) cannot be assured.

5.24 Security of Assets

It is accepted that, in order to provide healthcare services, the Trust's hospital sites are open to the public 24 hours a day 7 days a week and that, to be effective, equipment must be available and easily accessible by staff needing to use it. These requirements limit the level of security which can be applied to devices in areas which are open to the public.

5.24.1 Desktop Devices

This category covers a large number of different devices including (the list is not exhaustive):-

- PCs,
- Laptops,
- Printers,
- Thin Client devices,
- Scanners,
- Photocopiers,
- Projectors,
- DVD/Blu-Ray Players/Recorders,
- TVs

Devices should, where possible, be stored out of site of the public.

Computers in public areas should be risk assessed to determine their vulnerability. This should be done by the department to ensure unauthorised access cannot occur.

The contents of a computer can be protected through encryption if the device is an area open to the public;

The computer can be protected by means of a security cable or other such device, to an appropriate anchor point.

Specifically, laptops computers should be physically secured by a cable, due to the portability of the device.

If laptop computers are used in offices (which are not considered public areas) they should be locked with a security cable or must be locked away overnight. Laptop computers must not be left on a desktop overnight unsecured.

Staff working in public areas should challenge anyone, if safe to do so, if they see tampering with or attempting to remove equipment.

Printers, scanners and photocopiers which incorporate internal memory features should have these facilities disabled unless specifically required. If such facilities are used, care must be taken to clear the memory once documents held in it are no longer required. These devices should not be used as general document storage facilities.

DVD/Blu-ray players/recorders and TVs should be stored in locked cabinets where possible, or away from view in Lockable rooms.

5.25 Physical security and access

All staff must ensure they contribute towards maintaining physical security measures for data and access to data. These are in place to protect not only personal information but to also ensure the security of hardware and software. Where this it is likely that there may already be established security procedures in place however, these procedures need to be regularly reviewed and made available to staff or for staff to appropriately raise to management (if it is not their direct responsibility) so that remediation can be put in place.

There should be measures in place to delay and prevent unauthorised access, to detect attempted or actual unauthorised access, and to ensure that procedures are followed in the event that unauthorised access does occur (see reporting data breach on insite) This needs to be reported via email to the infogov email.

Managers should have procedures in place for staff to follow which are easily available and to support staff in knowing when to challenge unidentified visitors without visible trust ID especially in controlled areas, to know how to check that clinical room doors and blinds are closed or locked when not in use and in supervising collections/deliveries etc. These procedures should be readily available for staff to supplement the Data Protection training provided by the Trust. Staff will play a key role in ensuring the work environment is secure for fellow colleagues and patients by following these procedures to prevent unauthorised access.

Physical security measures must be applied to premises ensuring that

- Office doors are locked when the area is unmanned;
- Lock all consulting rooms and office areas when they are not in use.
- Windows in ground floor offices are locked;
- Blinds are drawn (where fitted) on ground floor offices overnight;
- Staff working in public areas should, if safe to do so, challenge anyone they see tampering with or attempting to remove equipment, inform the person in charge and call security for support if needed
- That equipment is not easily seen from outside.

5.25.1 Security of information

The provision of healthcare often involves constant use of confidential information In areas open to the public where it is vulnerable to unauthorised access. In addition, visitors, some temporary and contract staff, security and cleaning staff,

are examples of people with authorised access to secure, access controlled sites, who are not authorised to view confidential or sensitive data. The nature of the data and not site location dictates how and when this policy is applied. Where confidential (patient identifiable) or other sensitive (e.g. employee's pay scale) information is involved, users must, as and when appropriate: -

- Remove all sensitive information from the workplace and lock away, in a drawer or preferably in a fire resistant safe or cabinet. This includes all patient identifiable information, as well as other sensitive (personal or business) information such as salaries and contracts.
- Store visit, appointment or message books in a locked area when not in use.
- Angle computer screens away from the view of patients and visitors
- When leaving a workstation either log out or, in the case of a PC, lock the screen. (Press keys ctrl,alt,del at the same time, or the Windows key (next to alt) and L).
- Store paper and computer media in secure cabinets or safes.
- Locate photocopiers and printers so as to avoid unauthorised use.
- Ensure that post-it notes and sticky labels holding patient-identifiable or other sensitive information are not left to public view.
- Before a patient enters a consulting room, remove all evidence of the previous patient from view (computer screens, medical records, test papers or samples etc).
- In cases where patient information is held and where practical, this should be anonymised.
- The movement of paper records, particularly through public areas, should be minimised.

Reception desks and Nurses Stations can be particularly vulnerable to visitors. These areas should be kept as clear as possible at all times, in particular medical records should not be left open and with other patient identifiable information, should not be held on the desk or within reach/sight of visitors or patients.

5.25.2. Servers

Separate IM&T guidance exists for the security of servers and server rooms

5.25.3. Using removable media

Since UHL computers are all connected to a network which allows sharing of data within the Trust, if data is downloaded to removable media then this implies that information is going to leave UHL premises. This should be a rare occurrence so the use of removable media should be questioned. If there is a need to use removable media for personal or confidential data, the following must be adhered to:

- Memory Sticks, CDs, DVDs and any other removable storage device which contain Trust Data must be encrypted to Department of Health and Social Care (DHSC) standards.

- Confidential or personal data should only be written to encrypted memory sticks/pen drives which have been approved by IM&T. Colleagues are to email Infogov@uhl-tr.nhs.uk and complete a form to request a Memory Stick. The cost of the memory stick will be charged back to their department and is not for personal use.
- Any bulk extracts of confidential or sensitive data must be authorised by the responsible senior manager for the work area and request then sent to the Privacy Unit for their consideration.
- Staff who have been authorized to use removable media for the purposes of their job roles are responsible for the secure use of those removable media as highlighted in these guidelines. Failure to comply with this removable media policy may endanger the information services of UHL and will be investigated under HR policies.
- Removable media may only be used to store and share NHS information that is required for a specific business purpose. When the business purpose has been satisfied, the contents of removable media must be removed from that media through a destruction method that makes recovery of the data impossible. Alternatively the removable media and its data should be destroyed and disposed of beyond its potential reuse. In all cases, a record of the action to remove data from or to destroy data should be recorded in an auditable log file;
- Removable media should not be taken or sent off-site unless a prior agreement or instruction exists. A record must be maintained of all removable media taken or sent off-site, or brought into or received by the organization. This record should also identify the data files involved;
- Removable media must be physically protected against their loss, damage, abuse or misuse when used, where stored and in transit;
- Data archives or back-ups taken and stored on removable media, either short-term or long-term, must take account of any manufacturer's specification or guarantee and any limitations therein;
- All incidents involving the use of removable media must be reported to IT and through the Trust's incident reporting mechanism.
- Removable media must be returned to IM&T for destruction.

Line managers are responsible for:

- the day to day management and oversight of removable media used within their work areas to ensure this policy is followed;
- the secure storage of all unallocated removable media and its related control documentation as required by this procedure;
- ensuring that staff involved in data extraction and data file creation are fully aware of Trust policies, procedures and guidelines. (Note, e-learning entitled Cyber Security and Data Protection is available free of charge on the Trust E-Learning Suite HELM.)

5.26 Medical/Laboratory Equipment

This category constitutes all equipment, not included in the above categories, which is used within the Trust and which collects, stores, manipulates and/or produces information.

Users of such equipment must be aware that information stored within it may be of a sensitive nature. The following should therefore be considered when dealing with it:-

- When not in use, the equipment must be stored securely to prevent theft
- Information should not be held on the equipment for longer than is necessary.
- Staff using such equipment must not only be trained in its operation but also made aware of the information held on it to remove it (when no longer required).
- An understanding of the nature of information storage must form a part of the acceptance testing phase for any new equipment.
- When leaving a workstation either log out or, in the case of a PC, lock the screen (press keys ctrl, alt, del at the same time, or the Windows key [next to alt] and L), and remove smart card if used.

Equipment should not be taken off site (for example repair) when the device contains disk drives or memory cards.

Disposal of medical equipment must take into account the disk drives or memory cards in the equipment, which should be removed and before the equipment leaves site.

5.27 Disposal of equipment

Great care must be exercised when disposing of any equipment which has been used in the processing of information if there is any possibility that some information may remain in/on it. Users must contact IM&T service desk on X8000 for advice on disposal and if required to arrange collection of equipment.

In cases where the information is held electronically, reference must be made to IM&T for the appropriate action to be taken (Note – formatting a disk and/or overwriting a tape does not necessarily destroy the information held on it). IM&T will arrange for the physical destruction of the media

The disposal of computing equipment is covered by the WEEE (Waste Electrical and Electronic Equipment) regulations and must therefore be done in an appropriate and legal manner.

5.28 Shredding

In cases where information is held on hard copy (paper, film, etc.), when no longer required (see the Corporate Records Policy on Insite) the media must be shredded. Tthe shredding must be placed into confidential shredding bags/bins.

5.29 Offsite working

This section is to support staff who use UHL supplied mobile data devices or paper records at any site other than their normal place of work or at home, by ensuring

that they are aware of the information security issues. In order to protect staff and other people, organisational assets and systems, staff who work at home or other sites must take appropriate security measures to protect information and equipment. Please refer to the Agile Working (Including Home Working) UHL Policy in Section 9 for more information.

5.30 Physical Security in public areas / Access control

5.30.1 Usage in any public access area

The use of information in these areas must be kept to an absolute minimum, due to the threats of 'overlooking' and theft. Any member of staff choosing to use information and/or devices in these areas that results in any related incident will be required to state why the usage was required in that situation and the efforts they made to protect the information and any equipment

Equipment in use will not be left unattended at any time.

5.30.2 Usage in areas not generally accessible to the public

(including other NHS premises)

Staff are responsible for ensuring that unauthorised individuals are not able to see information, access systems or remove equipment or information. If equipment is being used outside of its normal location and might be left unattended, the user must secure it by other means (such as security cable, locked cabinet or room).

5.30.3 Occasional usage at home

It is recognised that staff will have to hold UHL information at home.

- Only members of staff are allowed access to information being used at home in any form, on any media.
- Use of any information at home must be for work purposes only
- Staff must ensure the security of information within their home. Where possible it should be stored in a locked container (filing cabinet, lockable briefcase). If this is not possible, when not in use it should be neatly filed and stored in a way that it is not obvious to other members of the household.
- Any personal/sensitive (inc. patient and staff information) or organisationally confidential information that has to be taken home must be within folders marked 'private and confidential' and other members of the household instructed not to look at it.
- Where colleagues are working from home, they may be entrusted with any patient related information and must ensure that they observe the same confidentiality policy when engaging with Trust related works at home

5.30.4 Using equipment supplied by the Trust

- Any member of staff allowing access by an unauthorised person, deliberately or inadvertently may be subject to the Trust's disciplinary proceedings.
- Trust equipment must not be connected to any phone line, internet connection or other computer other than where access is to the NHSnet or the Trust's network via a secure remote link (VPN). Staff working from home are encouraged to use a VPN link to securely access UHL systems.
- Any equipment supplied for remote access to NHSnet or the Trust must be stored securely when not in use. Where a system requires a PIN number and a 'security token' these must be stored separately
- The Trust's IT department is responsible for ensuring that access to supplied equipment requires a username and password and that anti-virus software is installed.
- For supplied equipment that is not classed as portable (i.e. a supplied desktop PC), the IT department are responsible for ensuring anti-virus software is regularly updated.
- Portable equipment (i.e. a laptops or similar devices), supplied by the Trust must be connected to the Trust's network every 60 days (maximum) for upgrade of anti-virus software and security updates. Failure to do so will result in the device being automatically disabled.
- Provided all policy statements above are applied, any supplied equipment may be used for any type of work which would normally be done on a UHL desktop PC. This includes the use of confidential information provided the general regulations on handling and storing confidential data are complied with.

5.31 Email and offsite working

The Trust has an e-mail policy to refer to but the following points apply directly to staff working from home.

5.31.1 Patient Identifiable Data Contained in an email

Patient or staff identifiable data must not be sent to a personal email address. Internet e-mail services of any sort are not secure and must not be used to send personal identifiable data or other confidential information.

5.31.2 Auto forwarding

Staff must not automatically forward their e-mail to a commercial ISP (Internet Service Provider) such as Hotmail to enable access at home.

Staff sending e-mail must be aware that it is not suited for confidential communications. Various systems are used for receiving e-mail and there is no guarantee that the addressee will be the only person to see the mail.

5.32 Transport of Equipment, Files and Paper Documents

When equipment, files and/or data are removed from Trust premises the individual removing them is responsible for ensuring its safe transport as far as is reasonably practical.

- Equipment, and paper files must be kept out of sight (in car boots), locked away and ideally not be left unattended at any time
- IT equipment must be transported in a secure, clean environment
- Appropriate packaging (such as sealed envelopes, bubble wrap etc) must be used to prevent physical damage
- Where a courier service is used to transport packages containing sensitive information tamper proof packaging must be used. Courier firms should guarantee the safe arrival of parcels and the confidentiality of any contained information through confirmation receipts. See the Safe Haven Policy B33/2011.

5.33 Disposal of media (electronic & paper)

Any disposal of media containing personally identifiable or organisationally sensitive information must take place on-site of the Trust in line with on-site disposal procedures. Staff with media to dispose of are responsible for returning it to site. Non sensitive information may be disposed of off site.

5.34 Disaster Recovery/Major incident planning

In the event of a major incident or disaster, the Trust may recall all equipment on loan to provide core services.

5.35. Awareness of this policy

This policy is available on the Policies and Guidelines Library, through the intranet and is referenced by a number of policies and guidance leaflets.

5.36. Contacts

- IM&T Helpdesk – 18000
- IT Training Department – 15662
- Information Governance Manager – 16053
- Technical Security Specialist – 15216
- Director of IM&T – 16782
- Head of Privacy- 26053
- Chief Inforamtion Officer- 27036

6 EDUCATION AND TRAINING REQUIREMENTS

Line Managers should ensure that colleague's access to HELM training for Cyber Security and Data Protection Training at the appropriate level to discuss how to

ensure Information is Secure and colleagues should apply this to their respective departments. Further support and clarification can be sought from Privacy Unit on 0116 2586053/8337

7 PROCESS FOR MONITORING COMPLIANCE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements Who or what committee will the completed report go to.
Systems Access Inventory	MBP/ IBM	MBP Internal Asset Tagging	Monthly	SIRO
Policy Review	Head of Privacy/Security Lead MBP	Risk & issues meeting	On anniversary date or as required	IM&T meeting and then Policy & Guidelines Committee

8 EQUALITY IMPACT ASSESSMENT

8.1 The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

8.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

This policy will assist the Trust in meeting its legal obligations in respect of EU directives and common law obligations as documented in the Information Governance Policy.

All policies and procedures developed relating to information will be designed to protect patients, staff and the Trust.

Other policies relevant to ensuring to confidentiality and integrity of information are:

- Data Protection and Confidentiality Policy A6/2003
- Health Records Management Policy B31/2005
- E-mail and Internet Usage Policy A9/2003
- Regulation of Investigatory Powers Act (2000)
- Human Rights Act (1998).
- Agile Working (including Home Working) UHL Policy B46/2020
- Mobile Device Management Policy B7/2007

Staff should also consider their UHL contract of employment

10 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts PAGL system.