Leicestershire Partnership
NHS Trust

Information Security and Risk Policy

This document describes the controls, processes and risk management put in place to maintain the confidentiality, integrity and availability of information stored and processed on Leicestershire Partnership NHS Trust IT infrastructure

Key Words:	IT, cyber, Information, security	
Version:	3	
Adopted by:	Trust Policy Committee	
Date this version was adopted:	7 October 2020	
Name of Author:	Head of Data Privacy/Data Protection Officer	
Name of responsible Committee:	Data Privacy Committee	
Please state if there is a reason for not publishing on website:	n/a	
Date issued for publication:	October 2020	
Review date:	March 2023	
Expiry date:	1 October 2023	
Target audience:	All Staff	
Type of Policy	Clinical ✓	Non Clinical ✓
Which Relevant CQC Fundamental Standards?	17 - Good Governance	

Contents

Version Control and Summary of Changes

Version	Date	Author	Status	Comment
0.1	Oct. 2001	Vicky Hill	Initial Draft	
0.2	Aug. 2002	Vicky Hill	Draft	Post Audit Review
0.3	Mar. 2003	Vicky Hill	Final Draft	For approval
0.4	Jan. 2008	Vicky Hill	Draft	Update in line with standard 27001. Plus introduction of encryption tools.
0.7	May 2010	Vicky Hill	Draft	Regular review
0.8	Nov. 2011	Vicky Hill	Final	TCS Alignment Information Risk/ Security and Recording policies. Inclusion of LPT RA policy and Access to systems policy. Expansion of e-commerce policy.
0.9	Oct. 2014	Vicky Hill		Review in line with ISP1
1.0	November 2016-17	Vicky Hill		Detailed review supporting ISP1 and ISO27001/2 2013
2.0	April 2018	Vicky Hill	Final	Amendments in line with changes in Data Protection Law and DSPT
3.0	July 2020	Head of Data Privacy	Draft	Full review including alignment with changes in the Data Security and Protection Toolkit and merger of various policies (Information Risk; IG Forensic Readiness) into one coherent policy

For further information contact:
Head of Data Privacy/Data Protection Officer, LPT-DataPrivacy@leicspart.nhs.uk

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all. This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Due Regard

LPT will ensure that Due regard for equality is taken and as such will undertake an analysis of equality (assessment of impact) on existing and new policies in line with the Equality Act 2010. This process will help to ensure that:

- **Strategies, policies and procedures and services are free from discrimination;**
- **LPT complies with current equality legislation;**
- **Due regard is given to equality in decision making and subsequent processes;**
- **Opportunities for promoting equality are identified.**

Please refer to due regard assessment (appendix 4) of this policy

Definitions that apply to this Policy

Anti-Virus	Software that provides an electronic defence mechanism mitigating the risk of a computing device being infected with or affected by malware.
Asset	Any information system, hardware, software, resource
Breach	Any event or circumstance that led to unintended or unexpected harm, loss or damage
Caldicott Principles	Set of Principles developed in the NHS relating to the management of patient information
Digital Evidence	Any digitally stored evidence which may be captured and used to support a specified investigation.
Electronic resource/Equipment	This includes computers (server, PC/workstation, laptop or any personal digital device), network assets, and any other peripheral equipment linked to the network, and also mobile phones and web enabled devices authorised for use for business which may not be linked to the network but could be used to send and receive text messages or other data
Firewall	A Firewall is security mechanism that limits access across a network connection
Forensic/Incident Investigation readiness	The collection of digital evidence to meet the business risk assessment, and in advance of any incident occurring
Hardware	Equipment concerning or connected to a computer is often referred to as hardware. This equipment is divided into two categories, hardware and peripherals. Hardware is the heart of any computer system enabling the processing and storing of electronic data. Hardware includes: • The base or tower unit of PC's – normally containing the processor and hard disk drive • Notebook or Laptop computers • Network servers • Removable or External Hard disk or Zip drives • Removable or External Tape drives. • Any other removable data storage devices • Smart devices (see hand held devices below)
Information Asset	A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.
Information Asset Owner	A named senior manager who is able to influence the SIRO and has responsibility for the security of identified assets
IT Security/Cyber	IT security/Cyber security is the body of technologies,

Security	processes and practices designed to protect networks, computers, programmes and data from attack, damage or unauthorised access. The overarching aim to ensure confidentiality, integrity and availability of data and IT systems.
Information Security Management System	A systematic approach to managing sensitive information relating to the business, so that it remains secure. It includes people, processes and IT systems by applying a risk management process.
Media	Removable digital, laser, magnetic, optical or paper based information store. Examples include: • Medical records • Letters, documents, computer print-outs • Floppy disks • Magnetic Tape – (incl. Audio, computer and video) • CD-R + CD-RW • USB drives Any other make/type of equipment meeting this criterion
Mobile Device	Any electronic device capable of creating, receiving, transmitting and storing portable data, with the ability to connect to, and exchange information with, a PC or laptop computer. This includes devices known as: • Hand Held computers • Smart phones and tablets (including ios and android devices) Any other make/type of equipment meeting this criterion
Monitoring	The interception of communications, monitoring systems, logging, recording, inspecting and auditing; and communication of this with nominated investigators to satisfy organisational responsibilities and obligations under the Law
Network	An infrastructure which is configured and maintained to assure performance, availability and integrity of information exchange between the computers and peripherals it connects.
Peripherals	Equipment connecting to hardware to enable input and output of electronic data; peripherals are often inter-changeable. They do not store data. Peripherals include: • Monitor • Keyboard • Mouse/Trackball • Scanner • Printer

	- Projector
Personal Confidential Data (PCD)	The Caldicott review interpreted '**personal**' as including the **Data** Protection Act **definition of personal data**, but included **data** relating to the deceased as well as living people, and '**confidential**' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' The GDPR's definition of personal data is now also much broader than under the DPA. Article 4 states that "'personal data' **means** any information relating to an identified or identifiable natural person ('**data subject**')".
Risk Management	The identification, assessment, and prioritization of risks. The level within the management hierarchy at which a risk is currently being managed at / has been escalated to
Senior Information Risk Owner (SIRO)	Director level manager who sits in the Board and is responsible for reporting information risk to the Board and Chief Executive
Software	Programs loaded onto hardware may enable the user to create process and store information. Software may require a licence. Software includes the operating system, Microsoft Windows and application suites such as Microsoft Office, which comprises Access, Excel, Outlook, PowerPoint and Word.
Surveillance	**Intrusive –** defined by RIPA as covert surveillance which is carried out in relation to anything taking place in any residential premises or in any vehicle and involves the presence of an individual on those premises. NHS bodies **cannot** undertake this type of surveillance. **Directed –** Defined as covert surveillance which is not obtrusive, and is undertaken for a specific investigation and in a manner likely to obtain private information about a person. This is relevant here, only in fraud related cases
System Security Policy (SSP) or System Level Security Policy (SLSP)	A security policy which is specific to a particular information system and meeting the requirements defined in the NHS Information Security Code of Practice

1.0. Purpose of the Policy

The aim of this policy is to establish an overarching framework, outlining the approach, methodology and responsibilities for Information security and risk that provides assurance that:

- IT resources, (including systems and the information contained within) are managed securely and consistently according to national/industry standard and corporately specified standards and practices.
- Members of staff are aware of their responsibilities concerning security of IT resources and confidentiality of information they use and that information security is an integral part of their day-to-day business.
- Safe and secure IT environments are provided for storage and use of the Trust's information and that information is accessible only on a 'need-to-know' basis.
- Information security risks are identified and controlled

2.0. Summary and Key Points

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Leicestershire Partnership NHS Trust by:

- Ensuring that all members of staff are aware of their roles, responsibilities and accountability and fully comply with the relevant legislation as described in this and other Data Security and Protection (Information Governance) policies.
- Working with other partners/agencies to develop collaborative approaches, systems and processes relating to information security.
- Describing the principles of security and explaining how they are implemented in the organisation. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the Trust a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the Trust.

3.0. Introduction

Leicestershire Partnership NHS Trust is a public body, with information processing as a fundamental part of its purpose. It is important, therefore, that the Trust has a clear and relevant Information Security and Risk Policy. This is essential to the Trust's compliance with data protection and other legislation and to ensure that confidentiality is respected.

Information is of greatest value when it is accurate, up-to-date and accessible from where and when it is needed; inaccessible information can quickly disrupt or devalue mission critical processes. This policy aims to preserve the principles of:

- ***Confidentiality*** – That access to data shall be confined to those with appropriate authority and protected from breaches, unauthorised disclosures of or unauthorised viewing.

- ***Integrity*** – That information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification and not allow unauthorised modification of data.
- ***Availability*** – That information shall be available, delivered to the right person, at the right time when it is needed and protected from disruption, loss and denial-of-service-attack

Information stored on IT systems of the Trust, together with the various applications provided by these systems, are increasingly valuable corporate assets and it is therefore essential that the Confidentiality, Integrity and Availability if all information stored and processed on Trust systems, together with the services provided by these systems, remains protected against known and emerging threats. The Trust's provision of healthcare must not be jeopardised through any breach, loss or unavailability of our Information Systems.

This policy includes all IT resources under the ownership of the Trust and applies to:

- All information (digital, hard copy, photographic or audio) collected, processed, stored, produced and communicated through the use of IT resources by or on behalf of the Trust.
- IT information systems owned by or under the control of the Trust
- The Trust's networks, infrastructure and websites.
- Any device or equipment that connects to the Trust's network which is capable of accessing, reproducing, storing, processing or transmitting information.
- To all users (including substantive employees, voluntary and bank workers, contractors – agency and sub-contract staff, locums, partner organisations, suppliers and customers) if the Trust IT resources and information contained within.

Information Security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the Trust is providing a secure and trusted environment for the management of information used in delivering it business.
- Clarity over the personal responsibilities around information security expected of staff when working on Trust business.
- A strengthened position in the event of any legal action that may be taken against the Trust (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security (including addressing requirements of the Data Security and Protection Toolkit (DSPT) and forms part of the Trust Information Security Management System (ISMS) that conforms to

ISO/IEC 27001).

- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

In the event of an outbreak of an infection, flu pandemic or major incident, the Trust recognises that it may not be possible to adhere to all aspects of this document and in such circumstances, staff should take advice from their manager and all possible action must be taken to maintain patient and staff safety.

4.0 Policy Quick Reference Guide

For quick reference the guide below is a summary of the expectations of this policy. This does not negate the need for all staff to be aware of the detail outlined but is intended to assist staff in understanding their roles and responsibilities at a glance.

1. The Trusts' IT resources are business tools and must be used responsibly, ethically, effectively and lawfully. You must be fully aware of the unacceptable uses defined in this policy and not engage in such activity at any time.
   Policy
2. The Trust employs systems to monitor use of its IT resources and, whilst conditional personal use of some IT resources is permitted, there must be no expectation of user privacy.

3. You are personally responsible for ensuring that no actual or potential security breaches occur as a result of your use of the Trust's IT resources. You are expected to:

   - Understand your responsibilities to prevent theft.
   - Protect and maintain the confidentiality and integrity of the Trust's data
   - Ensure operational security of information, equipment, networks and systems used

4. You must only use the user accounts that are assigned to you to access the Trust's network and IT systems. You must not use accounts of other authorised users or allow others to use your own accounts. This includes the use of smartcards to access Trust information systems.

5. You must only use Trust approved systems and solutions to share information, and only share that which is appropriate, relevant and authorised. Staff are to comply with Data Protection Law (General Data Protection Regulation – GDPR, and Data Protection Act 2018) and Caldicott Principles, never disclosing any Trust information to unauthorised recipients or those who do not 'Need-to-Know'.

6. All proposed changes to the Trust IT infrastructure and services (e.g. software

upgrades/installations and new IT services) must gain approval through the Software Approval Process before implementation.

7. You must comply with notifications that are issued by Leicestershire Health Informatics Service (LHIS) concerning collective or individual action that must be taken in response to potential or actual information security threats.

8. All staff should be cautious about any potential SPAM/unsolicited emails and delete any at the earliest possible opportunity and informing LHIS service desk.

9. No staff are to connect privately procured hardware to any of the Trust IT equipment or network without prior approval through the appropriate approval process.

10. No staff are to install any software on Trust IT equipment without the prior written approval.

11. You are responsible for the correctness and accuracy of data that you input into the Trust's IT systems (clinical and non-clinical), and it is expected that you understand the potential consequential effects of error. You must identify and correct errors promptly and report any loss or corruption of data that you find.

12. To ensure timely erasure of data, and secure disposal, you must return IT equipment that is redundant to LHIS for secure and confidential disposal of media.

13. All staff are to use complex passwords which are changed on a regular basis (maximum of 30 days).

14. All workstations should be locked or logged off when unattended.

15. Any member of staff observing an IT security incident must raise a report in accordance with the Trust Incident Reporting Policy (i.e. via Ulysses) and provide the LHIS Service desk with relevant details.

16. Failure to comply with the requirements of this policy or inappropriate use of resources controlled by this policy is a serious matter and may result in the rights to use Trust systems and/or resources being withdrawn, disciplinary action or prosecution under law.

5.0. Duties within the Organisation

5.1 The **Trust Board** has a legal responsibility for Trust policies and for ensuring that they are carried out effectively.

5.2 The **Trust Policy Committee** is mandated on behalf of the Trust Board to adopt policies

5.3 **Trust Board Sub-committees** have the responsibility for agreeing policies and protocols.

5.4 **Senior Information Risk Owner** (SIRO) is accountable for:

- Information risk within the Trust and advises the Board on the effectiveness of information risk management across the Trust;
- The Trust's information risk assessment process and information management;
- Overseeing adherence to this Policy to the satisfaction of the Trust;
- Ensuring documentation and appropriate action is taken where non-compliance to this policy or a need for improvement is identified.

5.5 **Caldicott Guardian** is responsible for:

- Ensuring implementation of the Caldicott Principles, National Data Guardian Standards and confidentiality and appropriate sharing of service user information throughout the Trust.

5.6 **Data Privacy Committee** is responsible for ensuring that this policy is:

- In accordance with data security and protection standards;
- Implemented and understood across the Trust

5.7 **Head of Data Privacy/Data Protection Officer** has responsibility for ensuring that Data Security and Protection standards are implemented effectively across the Trust. Including:

- The co-ordination, action planning and reporting of information security work and activity;
- Maintaining the Trust's Information Asset and data flow mapping registers and their regular review;
- Ensuring that investigation into all data loss is completed.

5.8 **Service Directors and Heads of Service are Information Asset Owners and System Managers** and are responsible for the protection, security and day-to-day management of designated assets/systems. Including:

- Development and enforcement of system security policies and appropriate operational and administrative procedures;
- The environments in which core and critical IT equipment are housed and information is processed and stored;
- The control and level of access (including privileged and administrative rights) granted to individual users of IT systems, networks and restricted areas housing core and critical IT equipment.
- Regular information security risk and vulnerability assessment and submission of results and mitigation plans to the SIRO;
- The development and maintenance of necessary business continuity and

disaster recovery plans and verification of their regular testing;
- Appropriate reporting, investigation and necessary remedial/corrective action relating to incidents, security breaches and data loss associated with respective information assets.

5.9 **Human Resources Department** is responsible for:

- Ensuring that information security requirements are addressed during recruitment and all contracts of employment contain appropriate confidentiality clauses;
- Information security responsibilities, duties and expectations are included within appropriate job descriptions, person specifications and HR policies and codes of conduct;
- Data Security and Protection (information security) awareness training is included in the Trust's staff induction process and annual mandatory training;
- Support the LHIS Cyber Security specialists in any IT Forensic investigations.

5.10 **Head of Leicestershire Health Informatics Service (LHIS)** is responsible for:

- Ensuring that the configuration and management of the Trust's IT equipment and networks is controlled through documented authorised policies and procedures based upon NHS and industry standards, best practice and recommendations;
- Authorising IT resources to be used by the Trust;
- Ensuring this policy is implemented and adhered to by the LHIS staff.

5.11 **LHIS and its staff** are responsible for ensuring the continuity and availability of Trust IT resources and the security and integrity of the data within its network. In addition to the other responsibilities and duties detailed in this policy, LHIS will:

- Ensure that all IT assets for which it is assigned responsibility are controlled by and subject to prescribed asset management procedures and processes;
- Ensure that IT equipment purchased on behalf of the Trust is added to the asset register, security labelled, protected and stored safely;
- Ensure IT equipment is appropriately configured for use and loaded with relevant licensed software;
- Allocate and configure individual user accounts and ensure associated user authentication of each authorised user of the Trust's IT resources;
- Provide and control external connections to the Trust's network in accordance with NHS standards and requirements;
- Ensure the removal of sensitive information and identity from the Trust's It equipment, its secure disposal and deletion from the asset register;
- Perform routine tests of disaster recovery procedures for core and critical IT equipment and key IT systems of the Trust;

- Ensure the provision of systems to monitor compliance with the Trust's IT policies and its legal and statutory obligations;
- Provide advice and guidance to users of the Trust's IT resources.

5.12 **Managers and Team leaders** are responsible for ensuring that their permanent and temporary staff and contractors have read and understood this policy and, in addition to the other responsibilities and duties detailed in this policy, that:

- Staff are instructed in their security responsibilities, work in compliance with this policy, related processes, guidelines and safe working practices;
- Staff are appropriately trained in the use of the Trust's IT resources and systems;
- Property registers in Electronic Staff Records (ESR) are kept up to date with IT equipment that has been assigned to staff;
- Agreements are in place with suppliers and external contractors that ensure staff and sub-contractors comply with appropriate policies and procedures before access to Trust systems or use of its IT resources is permitted.

5.13 **All Staff** are personally responsible for ensuring that no breaches of IT security result from their actions and shall:

- Comply with this policy, its related processes, guidelines and safe working practices;
- Ensure that they are fully aware of the unacceptable uses of IT resources as outlined in this policy;
- Understand their responsibilities to prevent theft, protect and maintain the confidentiality and integrity of the Trust's information assets and data and security of the Trust's networks;
- Ensure operational security of information and IT equipment and systems is used;
- Receive adequate training and/or guidance in the use of any IT equipment or systems provided by the Trust in relation to their own duties and responsibilities;
- Comply with notifications that may be issued from time to time by LHIS concerning any collective or individual action that must be undertaken in response to potential or actual information security threats;
- Understand their responsibilities to accurately enter data into IT systems and take appropriate action to identify and report missing, lost and incorrect data;
- Ensure that any incident that could potentially affect the security of information is reported in a timely manner.

5.14 **Other Authorised Users** of Trust IT resources are personally responsible for ensuring that no breaches of IT security result from their actions and shall:

- Comply with this policy, its related processes, guidance and safe working practices;
- Confirm such agreement in writing, via contract, memorandum of

understanding or other mutually agreed mechanism.

6.0 Policy Requirements

6.1 Use of IT Resources

The Trust's IT resources are business tools and users are obliged to use them responsibly, ethically, effectively and lawfully. Users of the Trust's IT resources shall comply with Trust policies, current safe working practices and NHS standards and best practice guidance.

Confidentiality and security clauses associated with the use of the Trust's IT systems, other IT resources and information contained within shall be appropriately included in terms and conditions of employment and addressed during recruitment.

Members of staff shall receive appropriate training in the use of the Trust's IT systems, other IT resources and personal security responsibilities before authorisation of their use is granted.

Members of staff provided with enhanced and privileged access rights (e.g. system and database administrators, Super Users, LHIS staff and similar) shall use their rights solely in the proper undertaking of their duties, and shall not deliberately access sensitive information without express and authorised permission.

With the exception of penetration and vulnerability testing that has been authorised by the SIRO, attempting to gain illegal or unauthorised access to data or systems, or seeking and exploiting weaknesses in IT systems or networks for unauthorised purposes, is a serious contravention of Trust policy and a criminal offence. It is strictly forbidden and is not tolerated under any circumstances by the Trust.

6.2 System Monitoring

In the interests of maintaining system security, complying with legal requirements, detecting and investigating unlawful activity and ensuring compliance with policies and standards is maintained, the Trust reserves the right to monitor use of its IT resources and information. This may include network access and activity, in-bound and out-bound traffic, device status and usage, session activity, password quality, e-mail usage, virus activity, web-browsing and critical event alerting.

Whilst conditional personal use of some IT resources owned by the Trust is permitted (e.g. email and internet), users should be aware that there must be no expectation of privacy. If privacy is expected, the Trust's IT resources must not be used for personal matters.

System monitoring reports will be provided as part of the cyber and information security metrics to the Data Privacy Committee for scrutiny and identification of any further actions, which may include awareness messages.

6.3 Information Risk

Information risk management is part of the Trust's overall risk management framework, as information risk should not be managed separately from other business risks, and will be considered as an element of the overall corporate governance framework.

In assessing the risks related to individual information assets priority must always be given to those that comprise or contain personal information about service users, their families, carers and staff.

The table below sets out the main groups of information assets that are considered within the reach Information Risk

Information Asset Description	**Type of Information Held**
Software	**Personal Information**
Applications and systems Data encryption Development and maintenance tools	Databases and data files, e.g. ESR Paper records, e.g. staff records, clinical records Paper reports, e.g. corporate records Audit data Back up and archive data
Hardware	**Other Information Content**
Computing hardware, e.g. servers, PCs, PDAs, Blackberries, IP Phones, laptops, removable media, cameras Network connections	Databases and data files e.g. ESR Audit data Back up and archive
Other Information Assets	**Other Information Assets**
Environmental services, e.g. power and air conditioning People skills and experience Shared services, including networks and printers Server rooms Training rooms and equipment Record libraries and archive stores	System information and documentation Operations and support procedures Manuals and training materials Contracts and agreements Business continuity and disaster recovery plans

Information risk is not the sole responsibility of IT or Information Governance staff. All staff have a responsibility to protect the security of confidential information particularly when it is person identifiable. All staff therefore should actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate action.

This requires a structured approach with the clear identification of specific roles and responsibilities to ensure that risks can be managed across all levels in the organisation. The Trust bases this approach on the clear identification of information assets. All information systems and equipment where data is held will be recorded on the Trust's asset register (database). Ownership for each asset is allocated to a senior accountable manager. Information asset administrator roles are allocated to operational staff with day to day responsibility for managing risks within their designated information asset. Administrators are supported where appropriate by the Health Informatics Service with responsibility for providing technical assistance on information risk management.

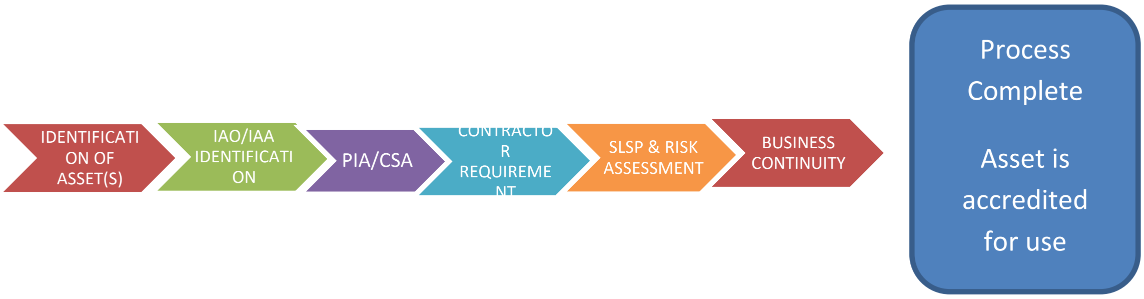
6.3.1 ***Information Asset Management***

The Information Asset Management Process is managed by the Head of Data Privacy in conjunction with Information Security personnel in LHIS. In order to give assurance that an asset is not going to be a major risk for the Trust a process of approval is in place, in line with national requirements, to ensure that assurance can be given that as a Trust we are ensuring the highest level of security and mitigating risk as much as is possible.

The process below gives an overview of how we ensure an asset is approved for use.

6.3.1.1 ***Asset Identification and Process***

Services need to begin preparation in identifying responsibility for service assets as the approval process develops; the Information Security personnel (LHIS) in conjunction with the Data Privacy Team will develop a programme of approval and will contact services to assist and support the process of ensuring assets already in situ within the Trust become approved for use.



1) Identification of Assets

The first stage in the process is the identification of the assets and the need for them to be approved for use. The Head of Data Privacy will register the assets on the Information Asset Register; this is the current register for all Trust assets.

The approval process in place will to help reduce the risks within the Trust and provide a mechanism for effectively identifying, mitigating and managing risks in relation to identified information assets.

2) IAO / IAA Identification

When an asset needs a review of its approval or a new asset is to be approved, the Data Privacy Team will liaise with the Information Security personnel in LHIS to assign a lead to help with the process. The first stage has to be the identification of responsibility and assigning an Information Asset Owner and Information Asset Administrator is essential.

3) DPIA / CSA

Data Protection Impact Assessment is required for new or changes to systems dealing with personal confidential data. Please see Privacy Impact Assessment Policy and Procedures for further details.

Clinical Safety Assessment - a form of risk assessment required for assets dealing with patient information, and undertaken by the clinical safety officer. IAOs / IAAs are required to consider and answer a set of questions to ensure the asset is not a risk to the safety of patient's and the data we hold and/or process about them.

4) Contractor Requirements (Where applicable)

It is essential to ensure that when an asset is approved for use that the correct checks are carried out to reduce the risk to the Trust by ensuring that any contractor is fit for purpose and can meet statutory and regulatory standards.

5) System Level Security Policy and Risk Assessment

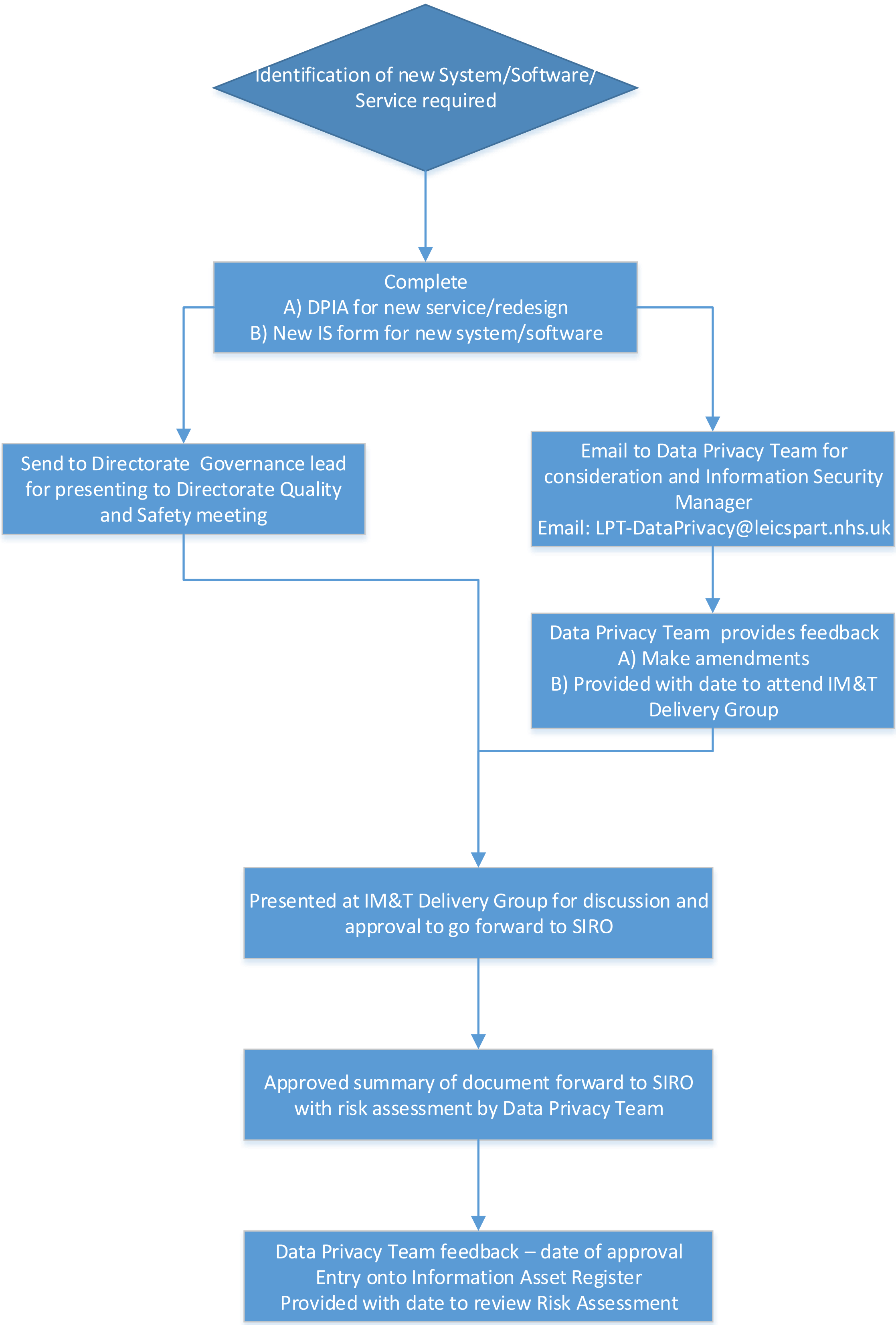
In order to further reduce and / or be able to manage risk within the approval process a System Level Security Policy is required to ensure that all aspects of security are considered.

The SLSP template can be requested from the Data Privacy Team via email: LPT-DataPrivacy@leicspart.nhs.uk

6) Business Continuity

The IAO's / IAA's are required to provide a Business Continuity Plan as this also assists the approval process to mitigate risks within the Trust. We can be confident that a service has thought about service provision if a system becomes unavailable.

During the process any risks identified need to be brought to the attention of the Senior Information Risk Owner (SIRO). The SIRO is presented with the information at the Executive Committee and assesses the information and ‘signs the information asset off’ as ‘approved for use’.


Identification of new System/Software/ Service required
Complete A) DPIA for new service/redesign B) New IS form for new system/software
Send to Directorate Governance lead for presenting to Directorate Quality and Safety meeting
Email to Data Privacy Team for consideration and Information Security Manager Email: LPT-DataPrivacy@leicspart.nhs.uk
Data Privacy Team provides feedback A) Make amendments B) Provided with date to attend IM&T Delivery Group
Presented at IM&T Delivery Group for discussion and approval to go forward to SIRO
Approved summary of document forward to SIRO with risk assessment by Data Privacy Team
Data Privacy Team feedback – date of approval Entry onto Information Asset Register Provided with date to review Risk Assessment

6.3.2 ***Contract Obligations***

The Trust will use the data handling clauses from the Office of Government Commerce ICT contract for services as its generic information governance model contracts for contracts with third parties.

If a contract is handling any personal identifiable / sensitive information a data processing agreement will be issued.

6.3.3 ***Adoption of Specific Action to Protect Patient Information***
The Trust places significant importance on the need to protect personal confidential data particularly where release or loss may result in harm or distress to the individuals concerned.

The Trust will therefore identify and manage risk in secure ways associated with the transfer of data to and from other organisations where release or loss could result in a breach of confidentiality or data protection. All personal data will be protected to the same level and will encompass as a minimum all data falling into the categories below:

- Any information that link one or more identifiable living person with information about them whose release would put them at significant risk, harm or distress. This includes all types of sensitive personal information (i.e. age, gender etc.).

The Trust undertakes an annual information flow mapping exercise and from this exercise to determine the information risks regarding its data flows within the organisation and with its delivery partners.

The Trust undertakes to minimise the risk from unauthorised access to protectively marked information. This includes holding and accessing data on IT systems in secure premises, secure remote access, reducing and avoiding the use of removable media apart from where it is in an encrypted form, ensuring that all portable computers are encrypted. It also includes ensuring the secure destruction and disposal of electronic and paper media through a clearly defined destruction policy and set of procedures which includes shredding, confidential waste removal erasure and degaussing.

Action is taken to minimise the risk prevented by unauthorised access to protect information. This will be achieved through a variety of measures, including:

- Enforcing stringent access controls to both electronic and paper information systems which hold person identifiable information.
- Having in place arrangements to log and audit activity of data users.

6.3.4 ***Vulnerability assessments (due diligence)***
There assessment are undertaken:

- To ensure that new IT infrastructure is installed in an appropriate secure manner and when existing IT infrastructure undergoes a significant change;
- For any new system providing access to the Trust's or NHS data;
- When there is a significant change to a system that could affect its security (e.g. change to authorisation/authentication mechanism, interface change, etc).

All users of the Trust's IT resources are personally responsible for ensuring that no actual or potential security breaches occur as a result of their actions.

Potential and actual information security breaches associated with the use of the Trust's information and IT resources shall be reported and investigated in accordance with the Trust's Incident Reporting Policy and procedures.

In instances where collection, preservation and protection of digital evidence is required for legal or disciplinary matters, the Cyber Security Team will be contacted at the earliest opportunity.

6.4 Incident Management

Information incident reporting is in line with the Trust's overall incident management reporting processes. Information incidents will be reported as soon as possible and recorded in accordance with the Incident Reporting Policy, on an e-IRF. In addition, information incidents should also reported through the LHIS Service desk to the LHIS Information Security Manager.

In particular, information incidents involving personal data are to be reported and managed in line with explicit guidance on the management of incidents involving personal data set out by NHS Digital via the Data Security and Protection Toolkit Incident Reporting Guidance.

6.4.1 ***Information Forensic Readiness***
Information Technology Forensics provides a systematic, standardised and legal basis for the admissibility of digital evidence that may be required to resolve formal disputes or support the legal process.

In the event of a suspicion that a computer or information system may have been used for a criminal or inappropriate purpose, persons appropriately trained and experienced in securing digital evidence from computers will be consulted in line with agreed procedures. The expert gathering of evidence will be undertaken by the authorised computer forensic investigators within by the Health Informatics Service.

This aspect of the Information Security and Risk Policy defines a systematic and proactive approach to the gathering and preservation of evidence to meet the business needs. This is complementary to and an enhancement of many existing information security activities undertaken and seeks to highlight the links.

There are established policies and procedures for Incident Management, escalation of Serious Incidents (SIs), and including fast tracking of incidents which require admissible digital evidence to be gathered.

The process is supported by an incident management team, human resource expertise, qualified and authorised computer investigation experts and support staff (acting under instruction), in ensuring that evidence found in an investigation is preserved and that the continuity of evidence is maintained.

6.4.1.1 Business Risk Assessment

The following business scenarios are identified as the key risk areas which may require digital evidence. These will be reviewed annually.

- Reducing the impact of computer related crime (including cyber crime, intellectual property protection, fraud, extortion, content abuse, privacy invasion and identity theft)
- Dealing effectively with court orders to release data
- Demonstrating compliance with regulatory or legal constraints
- Producing evidence to support disciplinary issues
- Supporting contractual and commercial agreements
- Proving the impact of a crime or dispute

6.4.1.2 Evidence Collection Requirement

Evidence collection requirements are confirmed in the System Security Policy (SLSP) specific to individual systems and agreed with the IAO and SIRO.

Where systems are outsourced or externally managed, assurances are sought and documented in the System Level Security Policy for the system.

Where evidence required is not currently collected, collection will be subject to a cost benefit analysis. The SLSP documents the system owner (IAO and IAAs) and the forensic readiness, monitoring, retention and storage arrangements for the system. There is a detailed security risk assessment which includes consideration of the wider business risks identified in this policy e.g. computer crime, fraud and the business scenarios identified as needing digital evidence.

Named managers with responsibility for security (IAOs and IAAs) review system details and assurances, including forensic readiness, regularly and report assurances, weakness and risks to the SIRO.

6.4.1.3 Capability for secure gathering

The capability for secure gathering of legally admissible data to meet the requirement is delivered by authorised and suitably qualified computer forensic investigators, supported by the LHIS.

6.4.1.4 Approach to Surveillance

Surveillance must not be considered without obtaining advice and guidance from the organisation's Local Counter Fraud or Local Security Management Specialist.

Any surveillance undertaken must be logged in a Surveillance Log.

6.4.1.5 Digital Evidence Usage

Preparation to use digital evidence may include

- Enhanced system and staff monitoring
- Technical, physical and procedural means to secure data to evidential standards of admissibility
- Processes and procedures to ensure that the importance and legal sensitivities of evidence is understood by staff
- Appropriate legal advice and interfacing with law enforcement.

6.4.1.6 Storage and Handling of Digital Evidence

Secure storage and handling of potential evidence, for example, that gathered through routine log files, or specific monitoring or surveillance activities will be

- Stored and handled with security measures that ensure the authenticity of the data
- Include procedures to demonstrate that the evidence integrity is preserved.

6.4.2 ***Managing Digital Evidence in Investigations***

Incident capture, investigation, escalation, storage and handling of potential evidence and incident review, includes referral to the police where required.

There is fast track reporting of incidents which may require digital evidence to be used, to the SIRO. Under director level instruction, advice is taken from an authorised computer forensic investigator who liaises with the Incident Lead, Human Resources, the Local security manager, and the Counter Fraud lead as appropriate.

Legal review is requested as necessary.

See Appendix 5 for the range of possible evidence sources

6.5 **Control and Management of IT assets**

All IT resources of the Trust (hardware, software, networks, systems or data) are the property of the Trust; they shall be recorded in appropriate asset registers and have a named information asset owner or system manager who is responsible for the control, management and security of that asset.

All IT resources of the Trust will be securely and appropriately configured and managed. The networks of the Trust are protected through the implementation of a set of well balanced technical and non-technical measures that provide effective and cost effective protection commensurate with assessed risk and vulnerabilities.

Unless approved by the SIRO, all systems procured for use by the Trust will comply with the minimum requirements set out within the relevant IT guidelines and be assessed to identify potential security threats, vulnerabilities and risks that might be introduced by their implementation.

System level security policies must be developed by information asset owners and system managers for all core IT assets and key IT systems.

The use of legacy hardware and software (that is products for which the vendor no longer provides support) shall be minimised and, where unavoidable, plans will be made to move to supported products as soon as possible. Where legacy products remain in operation the information asset owner or system manager shall regularly consult with LHIS technical teams to agree timely controls to be implemented to minimise risks that may occur from continuing usage (including ongoing monitoring effectiveness of implemented controls).

IT equipment owned and controlled by the Trust, and equipment that has been used for the storage of sensitive information, shall only be removed from its premises (temporarily or permanently) with prior, appropriate authorisation/documented release. Equipment will not be removed by a third party (e.g. the supplier, a repairer or disposal agent) until a signed confidentiality and transfer responsibility agreement has been exchanged or the equipment has been appropriately sanitised to remove all data.

In instances where IT (including removable media) equipment is to be allocated to a different user, or where it is to be repurposed, LHIS service desk shall be consulted to advise upon and carry out necessary clearing and sanitisation prior to reassignment.

At the end of life, all IT equipment (including removable media) owned or controlled by the Trust must be returned to LHIS for erasure of data and secure disposal in accordance with NHS standards and guidelines.

The Trust takes seriously its duties and obligations to use software responsibly, lawfully and in compliance with licensed terms and conditions. All software and systems used by the Trust will be:

- Properly licensed, and authorisation to use software and systems shall be dependent upon the availability of licenses;
- Used within the terms and conditions of the software license;

- Approved, tested, reliable and robust software that can be supported effectively by LHIS or a suitably qualified reputable third party supplier (only with the agreement of LHIS);
- Deployed or installed by LHIS or their authorised representative.

All changes associated with the deployment if new services, systems, software and IT solutions shall be subject to and managed via a formal and appropriately authorised change control procedure which may include the undertaking of a Data Protection Impact Assessment.

6.5.1 ***Personal Use of Trust owned Assets***

The following conditions apply to use of LPT IT equipment and services for personal purposes:

- IT equipment and services are provided primarily for use for Trust purposes. Management may authorise **limited** personal use as a benefit to staff, provided this does not interfere with the performance of their duties.
- Use of IT equipment and services for private work resulting in personal commercial gain is not permitted. (This does not apply to the provision of private healthcare services).
- The user must comply with this Policy. In particular, if taking equipment off-site, the user must comply with the rules for Agile Working policy.
- No information or software should be loaded which would compromise the use of equipment for work purposes.
- No software should be loaded onto trust equipment without express permission of the LHIS Infrastructure and Support Manager.
- Where the use of IT equipment and services for personal purposes is permitted, the user obtaining, recording or, storing information must do so in compliance with Data Protection Legislation; ensuring appropriate notification to the Information Commissioners Office where necessary. If you are unsure, please seek advise from the Head of Data Privacy.

6.5.2 ***Use of Non-NHS (e.g. user owned) Equipment***

- The connection of unauthorised devices on the network is prohibited.
- The use of non-NHS owned equipment and media for work purposes is not permitted.
- Where non-NHS devices are standalone equipment (not linked to the network) and with storage devices (including all forms of personal computers, smart devices, memory cards), or, where user owned software, is required to be used for work purposes, they must be authorised for use by the Head of Data Privacy and the Cyber Security Manager.
- The connection of non-NHS devices to the network is by exception and must be authorised in writing, by the LHIS Infrastructure and Support Manager. Telephone (0116 295) 3500 for advice.

- The use of equipment owned by non-NHS agencies (e.g. local government) will be risk assessed and due regard paid to the risks presented by the onward use and disposal of such devices subsequent to their use within the NHS;

- Where the use of non-NHS owned equipment is authorised, the user is reminded of their contract of employment obligations; namely that
    - Intellectual property rights of any development is as described in the contract.
    - NHS data will be removed from the device by the NHS at change of role, on leaving the organisation, or where the device is lost or stolen.
    - The organisation accepts no responsibility for private information which may be lost in ensuring secure removal of NHS information.
    - Non-NHS devices authorised for use for work purposes will be surrendered as required for the purposes of any audit or investigation undertaken by the Organisation.
    - The user is responsible for ensuring the physical protection of the device and that the device security is maintained up to date (e.g. accepting patches), and will comply with any technical configuration requests and procedures.

- Where authorised non-NHS owned devices which are smart phones and tablets, must be secured:
    - Password protection will be enforced.
    - Information will be passed to the device in an encrypted ‘bubble’
    - Loss or theft of the device will be reported immediately to the LHIS Service Desk so that NHS information can be remotely wiped.
    - When a user leaves the Trust, NHS information will be remotely wiped from the device.

Contact the LHIS Service Desk for more information

Personal confidential or other sensitive work related information must not be held on any other user owned equipment storage device or removable media as the Trust has no control over the future ownership of such equipment. If this information is inadvertently stored, the user should seek advice from the Service Desk for its removal (file deletion is not adequate).

6.6 **Access Control**

Access to the Trust’s IT resources and systems is restricted to users who have a justified business need to access the information contained within and are authorised by the relevant information asset owner or system manager.

Identification, authentication, passwords and/or smartcards are used to ensure access to the Trust’s systems, devices and information is controlled and restricted to authorised users only.

6.6.1 ***Access Management Control***

Access to Trust systems can be granted to the following types of individuals:

- Employees of the Trust – Staff directly employed by the Trust;
- External/Contract Employees – Staff employed by an external company and contracted to the Trust. This includes locums, secondees, students on placement, trainees and staff employed on the Trust's Bank;
- External Third-party support – Employees of external organisations that provide support for certain Trust systems may be granted restricted access;
- Access may be granted to others outside of the above categories in exceptional circumstances provided that there is a legitimate business requirement and that the access has been approved by the Head of Data Privacy or an appropriate deputy, with supporting Third Party Access Agreements in place.

6.6.2 ***User Account Types***

Access privileges, including enhanced and privileged rights, shall be based upon the function of the role and not status of the user's post. They will be modified or removed as appropriate when a member of staff changes their role or leaves the employment of the Trust.

There are various types of user accounts to support role function which are set out below:

- Standard: The most common type with restricted rights to install software, change settings or access privilege systems. Standard accounts must be used only by the individual that has been assigned to them. Sharing of usernames and passwords is a breach of data security and protection which will be reported and investigated and may be subject to disciplinary proceedings.

- Generic: An account that may be used by multiple individuals for a specific purpose. Due to the inability to effectively audit their usage generic accounts are only provided where there is a strong business related reason for them. Generic accounts will be highly restricted to allow only access to the resources needed to carry out their purpose. Access to the Internet, email and other areas open to abuse will be disabled or highly restricted as appropriate

- Temporary: A short-term account to be used by a named individual. Similar to a standard account, temporary accounts will only be considered where users only require access for no more than a month, there is a high turnaround of staff or where there is a legitimate reason for access at short notice. All temporary account users must have a User Account Form completed for standard user account access and this must be authorised by the authorising manager.
- Privilege: An account with elevated access rights to enable access to a specific system or systems to allow a user to carry out business functions.

- Administrator/Super User: A type of privileged account that is granted the highest level of access.

Generic, Temporary and Privileged account must be authorised by the Data Privacy Team or the Cyber Security Manager.

LHIS Information Security personnel will audit account types on a regular basis and may revoke access if deemed appropriate.

Remote access by third party suppliers of systems and software for support and maintenance purposes shall be subject to prior written agreement (either as part of a contract or specific separate agreement), and commitment to maintain confidentiality and integrity of the Trust’s information and data.

6.6.3 ***User Account Creation***

User accounts can only be requested by an authorising manager which is verified from the LPT IT Authorised Signatory list (managed by the Data Privacy Team).

Access to Trust systems will may be set to automatically expire at a given time where an expected end date is known. Expired accounts can only be re-enabled following a request from the authorising manager

All users will receive a Standard user account. By default this will have the following access:

- Email Account
- Internet Access
- StaffNet Access
- Personal Data Storage Area (H Drive)

Additional access rights to file share or to clinical systems etc must be requested separately by the authorising manager/sponsor.

If assigned as an owner to a resource (such as a shared network folder), it is the duty of that owner to be fully responsible for this resource at all times. They should ensure the correct staff members have permissions to access the resource and to transfer ownership to a new owner upon leaving their role.

In some instances, the owner of a resource may delegate the right to request additional access rights to appropriate staff. In these cases, it is the responsibility of the owner to ensure that the list of delegates is kept up to date and that they carry out regular (at least annual) audit of requests made by these delegates.

It is the responsibility of the authorising manager to ensure that their staff are familiar with this policy and any associated policies regarding the secure use of user accounts and equipment.

Staff user accounts will be assigned the name, job title etc that have been recorded by the Human Resources Department in the Electronic Staff Record (ESR). Where ESR has not been used to record all staff details (certain staff such as contractors are not always entered into ESR) the authorising manager must specify the required name when requesting access. Incorrect spelling of a name will result in a delay in the account being created or issues with the staff member logging in.

6.6.4 ***Changes to User Accounts***

Where ESR has been used as the source of the account name etc, then any changes to this information must be requested via the Workforce Information Team using the HR Change of Circumstances form.

All changes to accounts must be requested via the LHIS Service Desk or the LHIS Self Service Portal.

Staff changing job role, either permanently or as a result of secondment, must have their old access rights revoked and new access rights requested. It is the responsibility of both the previous authorising manager and the new authorising manager to ensure these requests are made via the LHIS Service Desk or LHIS Self Service Portal, as the changes made to ESR may not always be directly applicable to the user’s account details.

6.6.5 ***Disabling User Accounts***

As soon as an individual leaves the Trust all their access to Trust systems and buildings must be revoked.

LHIS will carry out regular audits of inactive accounts and disable those that have not been used within 90 days. If they have been inactive for legitimate reasons, they can be re-enabled at the request of the authorising manager.

A regular list of staff leavers will also be passed to LHIS via ESR. It is still the responsibility of the authorising manager to ensure that the user account has been disabled.

Where staff are absent for an extended period, such as maternity leave or long term sickness, it is the responsibility of the of the authorising manager to contact LHIS Service Desk so that the account can be disabled pending the staff member’s return.

When a user account is disabled, all current access rights will be removed. Disabled accounts must never be allocated to a new individual.

Disabled accounts will be archived to prevent resuse of the username. Associated data for the accounts will be retained and only be deleted in line with the Trust’s data retention policies.

6.6.6 ***NHS Smartcards***

Please refer to the LHIS Registration Authority Policy for more detail on the use and management.

6.6.7 ***Privilege Management***

Accounts with elevated privileges will be strictly controlled and only provided where there is a demonstrable business requirement for it.

A record of who has privilege accounts and the reason for those accounts will be maintained by the relevant system or service owner.

Privilege access will be audited on an annual basis or immediately following an incident where a privilege access played a role. The audit results will form part of the Cyber Security Managers Cyber and Information Security Report to the Data Privacy Committee.

Where privilege access is no longer appropriate it should be removed immediately.

Regular auditing of log files showing the use of privileged accounts will be carried out by the appropriate system owners or LHIS Information Security personnel.

6.6.8 ***Segregation of Duties***

Where practical segregation of duties should be enforced to minimise the opportunity for unauthorised, unintentional or malicious access, modification, or denial of service of the Trust's information security assets.

6.6.9 ***Access to Log Files***

Access to sensitive log files will be restricted to appropriate system owners, delegated admin teams and the LHIS staff.

Logs will be maintained in a secure environment that prevents unauthorised modification or deletion.

Regular audit of access to log files will be carried out and the outputs included in the Cyber and Information Security Reports to the Data Privacy Committee.

6.6.10 ***Disability Related Adjustments***

Should a situation arise whereby a user has difficulty authenticating because of a temporary or permanent disability, reasonable alternative processes may be considered, whilst still complying with the relevant security and governance standards.

To ensure that the Trust meets it obligations under the Equality Act, authorising managers should contact the LHIS Service Desk and Data Privacy Team to enable a solution which balances the needs of the individual with the Trust's legal requirements to Data Protection legislation.

6.6.11 ***Other Access Considerations***

- Access to and use of Trust's information in public areas and outside its premises is subject to additional measures of authentication, protection and requirements as specified in the Trust's Mobile and Remote Working guidelines.

- Only authorised personnel who have a justified and approved business need shall be given access to restricted areas of Trust buildings containing core and critical IT equipment. Staff entering and working in such areas will at all times comply with the Trust's current safe working practices associated with access to such areas.

6.6.12 ***Data and System Access***

Access to Shares, Public Folders, Shared Calendars and Shared Mailboxes will require authorisation from the owner or any assigned authorisers for that resource. For Global Distribution groups this can only be approved by Data Privacy Team who will support the identification of the owner of that group.

6.6.12.1 ***Staff Personal Drives and Mailbox***

Access to staff member's personal mailbox should be requested by the mailbox owner in the first instance or by a direct line manager if the owner is absent. Please note this only applies to Trust owned mailboxes. Access cannot be granted to non-Trust owned mailboxes. All requests to grant or revoke access must come via the Self Service Portal. All requests will be approved and managed by the LHIS Team in conjunction with the Data Privacy Team.

All data held on a user's personal drive on the Trust network is classed as 'live' data and access to this by another staff member must be approved by the Data Privacy Team in conjunction with LHIS Information Security. Due to the potential of a clinical risk or patient risk, no patient data of any kind (including data relating to a patient e.g. carer info) should be held on a personal drive. All patient and any other confidential Trust related data should be kept in the Trust networked shared drives or within the clinical system, accessible only by those authorised to see the data.

Access to live data held on a staff member's personal drive will only be granted in the following circumstances:

- The user has left the Trust and the account has been disabled via the LHIS Self Service Portal or the appropriate form (once the account is disabled the data is classed as historical)
- For the Information Security staff to get access to data required by another staff member

- For the Information Security staff as part of a formal investigation.

If specific data held on a staff member's personal drive is required, a request must be submitted to the LHIS Service Desk either via email or the Self Service Portal. The Information Security staff will arrange access to the H drive and will extract the specific data and move it to a specified location.

6.6.13 *General Guidance on the Secure Use of User Accounts*

- Accounts must only be accessed by the names individual to whom the account has been assigned;
- Service users must not be given access to any staff user account or devices attached to the Trust network, even under supervision;
- Sharing account login information is **prohibited** and **any** breach will be investigated by Data Privacy and Information Security personnel;
- Giving another person or persons access to your user account is **prohibited** and **any** breach will be investigated by Data Privacy and Information Security personnel;
- Login details must not be written down and stored in any location where they could be seen by an unauthorised individual;
- Passwords are changed every 30 days and meet complexity rules set out by the Trust;
- All unattended PCs or Laptops must be locked. In this context "unattended" means out of the user's direct line of sight;
- Admin/Super User accounts must have passwords that are changed regularly or when authorised staff leave or else be protected by an automated technical solution;
- Admin/Super User accounts should not be used for day to day business activities;
- Access rights should be granted using the principle of 'Least Privilege' to ensure that staff only have the rights they need to carry out their job role;
- It is the responsibility of the Information Asset Owner (IAO) of each system or Share to ensure that access rights for their system are managed appropriately and in line with the Trust policy and legal requirements;
- The authorisation and provision of access must be carried out by separate individuals to minimise the risk of abuse.

6.7 Systems, Databases and Application Development, Management and Maintenance

Local database or application creation or development must not be undertaken without prior consultation and agreement with LHIS and the Trust Data Privacy Team. Where agreement is given all database creation and development must align with the Trust's wide IM&T Strategy and comply with minimum standards for interoperability, data formats, capacity, auditing, performance and maintainability.

In house application development shall comply with the standards and working practices detailed in the relevant Trust IT guidelines.

Changes to IT systems shall be documented and assessed for their impact upon other systems prior to the change taking place.

All new releases of software applications and application developments shall be assessed in appropriate test environments prior to their release and be subject to satisfactory functional, non-functional and end-user-testing before being put into operational use.

Unless expressly and appropriately authorised, live sensitive information must not be used for testing, training or demonstration purposes unless it is transformed so that identification of any individual is not possible.

Live and test data shall be separated: If data is to be moved between live and test environments its migration shall be strictly controlled and subject to formal change control procedures.

Each IT system shall have a suitably trained administrator and documented operational procedures in place together with appropriate maintenance agreements.

6.8 Equipment Protection and Security

All IT hardware, software and systems purchased must comply with standards as defined in IT guidelines at the time of purchase.

IT equipment and systems not purchased through LHIS will not be connected to the Trust's network until it has been through testing and appropriate authorisation gained for connection.

Portable equipment (including removable media) shall be subject to the additional measures of protection and requirements as specified in the Trust's Remote and Mobile Working Guidelines.

6.8.1 ***Network Security***

To minimise the risk of date leakage and malware propagation, network segregation will be carried out using technology such as VLANS (Virtual Local Area Networks).

Individual systems may be isolates from the wider LAN to ensure that they meet internal, external or statutory security requirements.

VLANs will be managed by appropriately authorised LHIS staff

The Network Security Policy provides further details

6.8.2 ***Physical Security***

- IT equipment will be sited where reasonably practicable to reduce risk from environmental threat and unauthorised access. Where equipment is kept or installed in public areas of Trust buildings, it will be positioned as far as reasonably practicable, to reduce risk of unauthorised access or casual viewing.

- Reasonable and appropriate measures shall be taken to minimise the risk of theft of the Trust's IT equipment including the secure anchoring of equipment in public areas.

- Environmental controls and monitoring systems that trigger alarms should problems occur shall be installed to protect the Trust's core and critical IT equipment.

- Ingress/Egress rights must be assigned to an individual via the use of a token such as a smartcard, fob or other physical object.

- Visitors will be provided with visitor badges for the duration of their visit and may be granted rights to non-sensitive areas at the discretion of the authorising manager and the LHIS Information Security Team.
- Visitors **must not** be left unattended at any time in secure areas.

- It is the responsibility of the last person leaving a secure area to check that all the windows and doors are locked and that any alarm is activated.

- In the event of long term absence, such as sickness or maternity leave, it is the responsibility of the authorising manager to ensure that physical access rights have been revoked pending the staff member's return.

- Access to areas housing the Trust's core and critical IT equipment will be restricted and kept secured at all times.

- Where possible core and critical IT equipment of the Trust shall be connected to secured power supplies, using uninterruptible power supplies and generator backup services to ensure that it does not fail during failure of the mains supply or switchover between mains and generated supplies.

- Uninterruptible power supplies shall be dimensioned to ensure that relevant equipment and key IT systems can be shutdown by controlled processes in the event of continuing supply failure.

- IT and communications cabling shall be protected from interception or damage (via physical fabric of the building or in conduit) and sited in accordance with relevant standards in relation to electrical and heating services.

6.9 Remote Working

Staff have the ability to access the network using corporate Wi-Fi from various locations across Leicester and Leicestershire or, via the internet using a secure remote access (VPN) solution, which is facilitated through the use of secure encrypted devices (smart phones/tablets/encrypted laptops).

6.9.1 *Authorisation*

- Authorisation is required by a line manager that as part of your role there is a requirement to take information software, processing equipment capable of storing work related information outside of the organisation (e.g. laptops, tablets, memory cards, digital recorders, cameras, etc);
- There are team specific rules for office and off-site working patterns confirmed with the line manager;
- Where equipment used for off-site (or at home) is damaged/lost, the cost of rectification will be discussed with the user and associated budget holder;
- The use of IT equipment and services for private work resulting in personal commercial gain is not permitted (this provision does not apply to private healthcare services).

6.9.2 *Protection of Information and Equipment*

Portable equipment is a prime target for thieves and where it's loss includes sensitive information, the cost in public confidence is high.When using any type of mobile device or removable media, be vigilant – keep it safe!

Use approved NHS laptops, mobile devices and media only.

Smart Devices used for work purposes will be:

- Encrypted to NHS Standards
- Pin or password enforced
- Configured to prevent the storage of sensitive information in 'the cloud'
- Configured to access the secure corporate Wi-Fi
- Configured to permit remote wipe in case of loss, theft, repair, end of life
- Secured for onward use
- Disposed of securely at end of life

If your smart device is lost or requires repair or replacement contact the LHIS service desk on 0116 295 3500.

6.9.3 *Logical Security*

- Apply the rules for password or pin protection;
- Use the VPN solution for secure remote access;
- Use Ctrl Alt Delete to lock your device from view;
- Sensitive information, stored on removable media, laptop, or sent by email must be encrypted;
- If faced with sending unencrypted personal confidential data by electronic

means, you must have approval. Contact the LHIS service desk for options;

- Never carry your smartcard, or access details with your mobile devices;
- Do not store confidential or sensitive work information on non-NHS or unsecured equipment or media;
- The use of non-NHS equipment or media is exceptional and must be approved by the Data Privacy Team and secured in the LHIS secure devices solution;
- Contact LHIS service desk if NHS data is stored in error on non-NHS equipment;

<u>In transit</u>

- Keep your portable equipment with you when travelling;
- If left in the car, it must be locked in the boot;
- Beware thieves in airports, conference venues etc;
- Avoid work on confidential/sensitive information on trains or planes etc;
- Guard against confidentiality breach when using a smart device;
- Store manual records securely – fasten holders and bags;
- Protect equipment from the elements and electromagnetic fields

<u>Working away from the Office</u>

- In all locations, protect information from view by unauthorised people;
- For each session before printing, send a test print to confirm your printer location;
- Collect prints immediately;
- At home, log off or lock your equipment when you leave it;
  Elsewhere, never leave the equipment unattended;
- Store records, equipment and media safely when not in use;
- Store keys, smartcard, VPN Code receiving device separately from your laptop;
- At home use lockable storage or store out of sight, preferably upstairs
- Position equipment away from prying eyes, ground floor windows and sources of heat or dampness;
- Return all waste documentation, printouts and removable media to the workplace and follow the usual disposal procedures.

6.9.4 ***Backups, Software, Virus Protection***

- Data should be stored in an application system or on the network for assured backup;
- Always ensure that the latest version of work related data is stored on the network as opposed to the ‘C’ drive of your device;
- Only authorised software may be loaded onto a device. Contact LHIS service desk for advice;
- Software supplied must not be copied;
- A virus may cause serious disruption to all systems. Do not plug in or upload any unauthorised software or device;
- Never forward a virus warning, as they are often hoaxes;
- Report suspected viruses to the Service Desk;

- Login regularly to keep your anti-virus protection up to date;
- Ensure smart device security by accepting supplier security patches and software/updates.

Further information on working in an Agile way can be found in the Trusts' Agile Working Policy.

6.10 Information Storage and Sharing

Sensitive information shall:

- Only to be stored on Trust owned or controlled IT resources or authorised systems;
- Not to be intentionally placed on personal or privately owned devices and storage resources;
- Only to be sent outside the Trust with the authorisation of an appropriate Trust representative.

Staff shall only share information that is appropriate, relevant and authorised. Information that is shared electronically shall only be shared using Trust approved systems and solutions.

Information shall only be shared via email in accordance with the criteria and conditions detailed in the Trust Internet and E-Communications Policy, and Use of Electronic Communications with Service Users Policy.

Portable and removable media shall only be used to share information where secure direct transfer methods are not available, and under the following conditions:

- That it shall be in accordance with the requirements of the Trust's Remote and Mobile Working Procedures and associated IT Guidelines;
- That it is encrypted in accordance with NHS standards and guidelines;
- That, if not being transported personally by an authorised representative of the Trust, it is sent by a Trust approved courier or special (registered) delivery and confirmation of receipt must be obtained by the sender.

6.11 Operational Management and Procedures

Core and Key IT systems and services shall be backed up according to an appropriate schedule to ensure that business and operational functions of the Trust are not jeopardised and that data is retained for adequate intervals before being overwritten.

Back-up media shall be:

- Reputable and high quality media and devices;
- Clearly labelled and securely stored/located separate from the system location to protect against building loss.

Restoration processes shall be adequately documented to enable other (suitably qualified) staff to understand and employ them.

Backup data and restoration processes shall be regularly tested to ensure that they are effective.

Appropriate boundary protection controls and secure configuration techniques shall be used to ensure that:

- IT systems, devices and software are successfully and securely configured and locked down;
- Gateways are successfully and securely managed;
- Networks are securely designed and effectively monitored and incidents are promptly responded to.

Appropriate cryptographic controls that comply with NHS national standards and requirements will be used to ensure the integrity and confidentiality of communication, processing and storage of the Trust's information.

To ensure that risk disruption is maintained at an absolute minimum, all data residing on the Trust's network or flowing from it shall be protected against virus, malicious and mobile code software attack and cyber attack.

All IT equipment (including portable equipment and removable media) should be scanned for viruses and malware before being connected to other Trust equipment or its network.

IT equipment and systems infected with viruses or malware that protective measures have not been able to deal with shall be quarantined by LHIS until they are virus free.

Operating systems, core and critical software, key applications and firmware shall be regularly updated with published security patches.

6.12 Business Continuity Planning

Business continuity and disaster recovery plans shall be put into place and regularly tested for all mission critical IT systems, applications and networks.

Where possible and practicable, IT systems shall be designed to include controls that check for data corruption that has resulted from processing errors or other possible deliberate acts.

7.0 Training needs

There is a need for training identified within this policy. In accordance with the classification of training outlined in the Trust Learning and Development Strategy this training has been identified as mandatory and role development training.

8.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
16	Members of staff will receive appropriate training	Sec 6.1	Data Security Awareness Training compliance	Data Privacy Committee	Quarterly
17	System monitoring reports	Sec 6.2	Included in the Cyber and Information Security Reports	Data Privacy Committee	Quarterly
19	Asset Approval Process in place	Sec 6.3.1.1	Software approvals presented	IM&T Delivery Group	As Required
20	Business Continuity Plans in place	Sec 6.3.1.1	Confirmation as part of DSPT requirement	Data Privacy Committee	Annually
22	Contract obligations Due Diligence undertaken	Sec 6.3.2	Confirmation as part of DSPT requirement	Data Privacy Committee	Annually
22	Data Flow mapping undertaken	Sec 6.3.3	Reports presented as part of assurance work for DSPT	Data Privacy Committee	Annually
23	IT Incidents reported in line with Incident Reporting Policy	Sec 6.4	Number of IT reported incidents included in Cyber and Information Security Reports	Data Privacy Committee	Quarterly
27	Personal use authorisations	Sec 6.5.1	Numbers of requests included in Cyber and Information Security Reports	Data Privacy Committee	Quarterly
30	User Account Audits undertaken	Sec 6.6.2	Outputs of Audit included in Cyber and Information Security Reports	Data Privacy Committee	Quarterly
32	Disabling Accounts	Sec 6.6.5	Numbers of accounts disabled included in Cyber and Information Security Reports	Data Privacy Committee	Quarterly

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
32	Privilege Account Requests	Sec 6.6.7	Number of Privilege Account requests included in Cyber and Information Security Reports	Data Privacy Committee	Quarterly
33	Audit of Log Files is undertaken	Sec 6.6.9	Outputs of Audit included in Cyber and Information Security Reports	Data Privacy Committee	Quarterly

9.0 Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
CQC Regulation 17 Good Governance	Submission of Standards Met for Data Security and Protection Toolkit on an annual basis

10.0 References and Bibliography

The policy was drafted with reference to the following:

Internet and Electronic Communications Policy v2.0
Incident Reporting Policy v9.0
LHIS Network Security Policy
LHIS Registration Authority Policy
Agile Working Policy

National Data Guardian Standard 2017
General Data Protection Regulation (EU) 2016/679
Data Protection Act 2018
Regulation of Investigation Powers Act 2000

Appendix 1

Training Requirements

Training Needs Analysis

Training topic:	Data Security Awareness Level 1
Type of training: (see study leave policy)	x Mandatory (must be on mandatory training register) ☐ Role specific ☐ Personal development
Division(s) to which the training is applicable:	x Adult Mental Health & Learning Disability Services x Community Health Services x Enabling Services x Families Young People Children x Hosted Services
Staff groups who require the training:	All Staff
Regularity of Update requirement:	Annually
Who is responsible for delivery of this training?	eLearning via ULearn
Have resources been identified?	Yes
Has a training plan been agreed?	Yes
Where will completion of this training be recorded?	x ULearn ☐ Other (please specify)
How is this training going to be monitored?	Monthly training reports to Managers

Appendix 2

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	□
Respond to different needs of different sectors of the population	□
Work continuously to improve quality services and to minimise errors	x
Support and value its staff	x
Work together with others to ensure a seamless service for patients	□
Help keep people healthy and work to reduce health inequalities	□
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	x

Appendix 3

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Chris Biddle	Cyber Security Manager LHIS
Afroz Kidy	Security, RA and Assurance Manager LHIS

Circulated to the following individuals for comment

Name	Designation
Members of Data Privacy Committee	
Members of IM&T Delivery Group	
Dani Cecchini	Exec Director Finance, Business and Estates/Deputy CEO/ SIRO
David Williams	Director of Strategy & Business Development
Dr Girish Kunigiri	Consultant Psychiatrist/Chief Clinical Information Officer
Dr Avinash Hiremath	Medical Director/Caldicott Guardian
Haseeb Ahmad	Head of Equality, Diversity & Inclusion

Appendix 4

Due Regard Screening Template

Section 1	
Name of activity/proposal	Information Security and Risk Policy
Date Screening commenced	27 July 2020
Directorate / Service carrying out the assessment	Data Privacy Team Finance, Business & Estates
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland Head of Data Privacy/Data Protection Officer
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: To provide staff guidance in managing and handling Trust information assets	
OBJECTIVES: To establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Leicestershire Partnership NHS Trust	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Neutral
Disability	Positive – Section 6.6.10 outlines specific support to those with a disability and requiring additional resources
Gender reassignment	Neutral
Marriage & Civil Partnership	Neutral
Pregnancy & Maternity	Neutral
Race	Neutral
Religion and Belief	Neutral
Sex	Neutral
Sexual Orientation	Neutral
Other equality groups?	

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please <u>tick</u> appropriate box below.			
Yes		No	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	✓

Section 4			
If this proposal is low risk please give evidence or justification for how you reached this decision:			
The policy is aimed at all staff and sets out the specifically support to those with a Disability in order that they can fulfil their day to day duties			
Signed by reviewer/assessor	Sam Kirkland	**Date**	06/08/2020
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed	Sam Kirkland	**Date**	11/08/2020

Appendix 5

DATA PRIVACY IMPACT ASSESSMENT SCREENING

Data Privacy impact assessment (DPIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet Individual's expectations of privacy.
The following screening questions will help the Trust determine if there are any privacy issues associated with the implementation of the Policy. Answering 'yes' to any of these questions is an indication that a DPIA may be a useful exercise. An explanation for the answers will assist with the determination as to whether a full DPIA is required which will require senior management support, at this stage the Head of Data Privacy must be involved.

Name of Document:	Information Security and Risk Policy	
Completed by:	Sam Kirkland	
Job title	Head of Data Privacy	**Date** 06/08/2020

Screening Questions	**Yes / No**	**Explanatory Note**
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	Y	Where a new system or software is procured but there is an approval process in place to assess the risk to data privacy and security
2. Will the process described in the document compel individuals to provide information about them? This is information in excess of what is required to carry out the process described within the document.	N	
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	Y	Dependent on requests made but there are processes in place to assess the risk before agreement for the data flow
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Y	Where a new system or software is procured but there is an approval process in place to assess the risk to data privacy and security
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	Y	Where a new system or software is procured but there is an approval process in place to assess the risk to data privacy and security
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	Y	Dependent on requests made but there are processes in place to assess the risk before agreement for the data flow
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	Y	Dependent on requests made but there are processes in place to assess the risk before agreement for the data flow
8. Will the process require you to contact individuals in ways which they may find intrusive?	Y	It is possible dependent on requests made but there are processes in place to assess the risk before agreement for the data flow

If the answer to any of these questions is ‘Yes’ please contact the Data Privacy Team via Lpt-dataprivacy@leicspart.secure.nhs.uk **In this case, ratification of a procedural document will not take place until review by the Head of Data Privacy.**	
Data Privacy approval name:	**Sam Kirkland, Head of Data Privacy/Data Protection Officer**
Date of approval	**11/08/2020**

Acknowledgement: This is based on the work of Princess Alexandra Hospital NHS Trust

Appendix 6

Information Forensic Investigation – range of possible sources of evidence

- Equipment such as routers, firewalls, servers, clients, portables, and embedded devices;
- Application software, such as accounting packages for evidence of fraud, ERP packages for employee records and activities (e.g. in case of identity theft), system and management files; Plus documents and data necessary to comply with legal or regulatory requirements.
- Monitoring software such as Intrusion Detection Software, packet sniffers, keyboard loggers, and content checker;
- External storage media / removable media
- General logs, such as access logs, printer logs, web traffic, internal network logs, Internet traffic, database transactions, and commercial transactions, email traffic.

All but the simplest of computer systems require a password or authenticating device before allowing admission. Usually, these access control systems can be configured to maintain records of when usernames and passwords were issued, when passwords were changed, when access rights were changed and/or terminated. In addition, many systems also maintain logs of accesses or, at the least, of failed accesses. These logs, properly managed and preserved, are powerful evidence of tracking activity on a computer system.

All computers contain files which help to define how the operating system and various individual programs are supposed to work. In the current generation of Windows systems, the most important set of configuration information is the registry. From this, forensic technicians can discover a great deal about recent and past activity, including recently accessed files and passwords. Often, there are important configuration files associated with individual programs. Many operating systems also generate error and other internal logs.

- Other sources, such as CCTV, door access records, phone logs, PABX data, telco records and network records, call centre logs or monitored phone calls, and recorded messages; cell phones, PDAs (These last can hold substantial amounts of data. Technical methods for preserving and investigating them are more complex than those for PCs; in addition there may be additional legal problems as ownership and privacy rights may not be wholly clear)
- Back-ups and archives, for example, laptops and desktops; If individuals are under any form of suspicion, the organisation will need to be able to seize their PCs and make a proper forensic “image”, which produces a precise snapshot of everything on the hard disks (this includes deleted material which technicians may be able to recover).