NHS
Leicestershire Partnership
NHS Trust

Information Risk Policy

This policy lays the framework for a formal risk management programme in the Trust by explicitly establishing the accountability and responsibility arrangements for information risk identification and analysis, planning for information risk, mitigation, and the oversight of information risk management.

Key Words:	*Risk identification*	
Version:	3.0	
Adopted by:	Quality Assurance Committee	
Date Adopted:	20 February 2018	
Name of Author:	Head of Information Governance	
Name of responsible Committee:	Records and Information Governance Group	
Date issued for publication:	February 2018	
Review date:	August 2019	
Expiry date:	1 December 2020	
Target audience:	All Staff	
Type of Policy	Clinical ✓	Non Clinical ✓
Which Relevant CQC Fundamental Standards?		

Contents

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
1.0	March 2014	First Draft
1.0	May 2014	Amendments made following consultation
1.1	June 2014	Final following Policy Group for adoption
2.0	October 2017	Superficial changes only following review of policy
3.0	February 2018	Reviewed policy due to expiry date

For further information contact:

Head of Information Governance
0116 295 0997

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.

In carrying out its functions, LPT must have due regard to the different needs of different protected equality groups in their area.

This applies to all the activities for which LPT is responsible, including policy development and review.

Due Regard

LPT must have **due regard** to the aims of eliminating discrimination and promoting equality when policies are being developed. Information about due regard can be found on the Equality page on e-source and/or by contacting the LPT Equalities Team.

Definitions that apply to this Policy

Information	Facts provided or learned about something or someone
Information Asset	A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.
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'**)".22 Jun 2017
Privacy Impact Assessment	A process which helps an organisation to identify and reduce the privacy risks of a project.
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

1.0 Purpose

The purpose of this policy is to formally establish the Trust's position regarding an information risk management process. The intent is to embed information risk management into the business processes and functions by means of key assurance, review and control processes.

In doing this the policy supports the Trust's strategic business objectives and should enable staff across the organisation to identify an acceptable level of risk beyond which escalation of risk management decisions is necessary. The information risk policy therefore fits within the Trust's overall risk management framework. Information will not be managed separately from other business risks and will be considered as an element of the overall corporate governance framework. The information risk management policy has been developed in order to:

- Define how the Trust and its partners will manage information risk and how risk management effectiveness will be assessed and measured.
- Protect the Trust from those information risks of significant negative likelihood and consequence which may impact on its ability to deliver its stated strategic aims and objectives.
- Provide a consistent information risk management framework through which information risks relating to business processes and functions within the Trust can be identified, assessed, and addressed through the systems of review, control and assurance.
- Promote proactive rather than reactive approaches to information risk management.
- Meet statutory and NHS policy and strategic requirements.
- Assist in safeguarding the Trust's information assets which comprise of people, finance, property and reputation.
- Assist in the maintenance of respect for patient dignity and privacy through safeguarding uses of and accesses to patient data.

2.0 Summary and Key Points

This policy sets out the Trust's Information Risk Management Policy. The policy lays the framework for a formal information risk management programme in the Trust by explicitly establishing the accountability and responsibility arrangements for information risk identification and analysis, planning for information risk, mitigation, and the oversight of information risk management.

This policy complements the Trust's Risk Management Strategy and therefore the responsibilities, definitions and processes contained within the Risk Management Strategy apply to this information risk policy.

This policy also relates to the management of risk within all Trust systems which involve the collection holding and production of data whether this is in electronic or paper format and it relates to all types of data storage, audio, visual or data.

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

3.0 Introduction

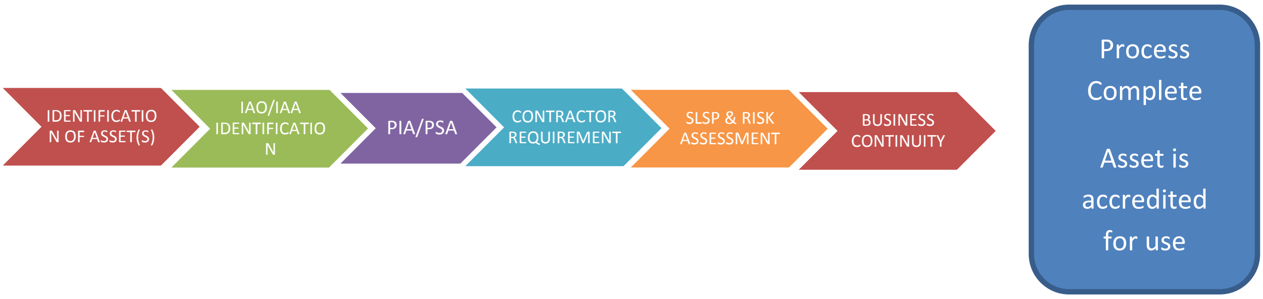
Information risk is inherent in all Trust activities. It refers to the on-going process of identifying information risk and implementing plans to manage them.

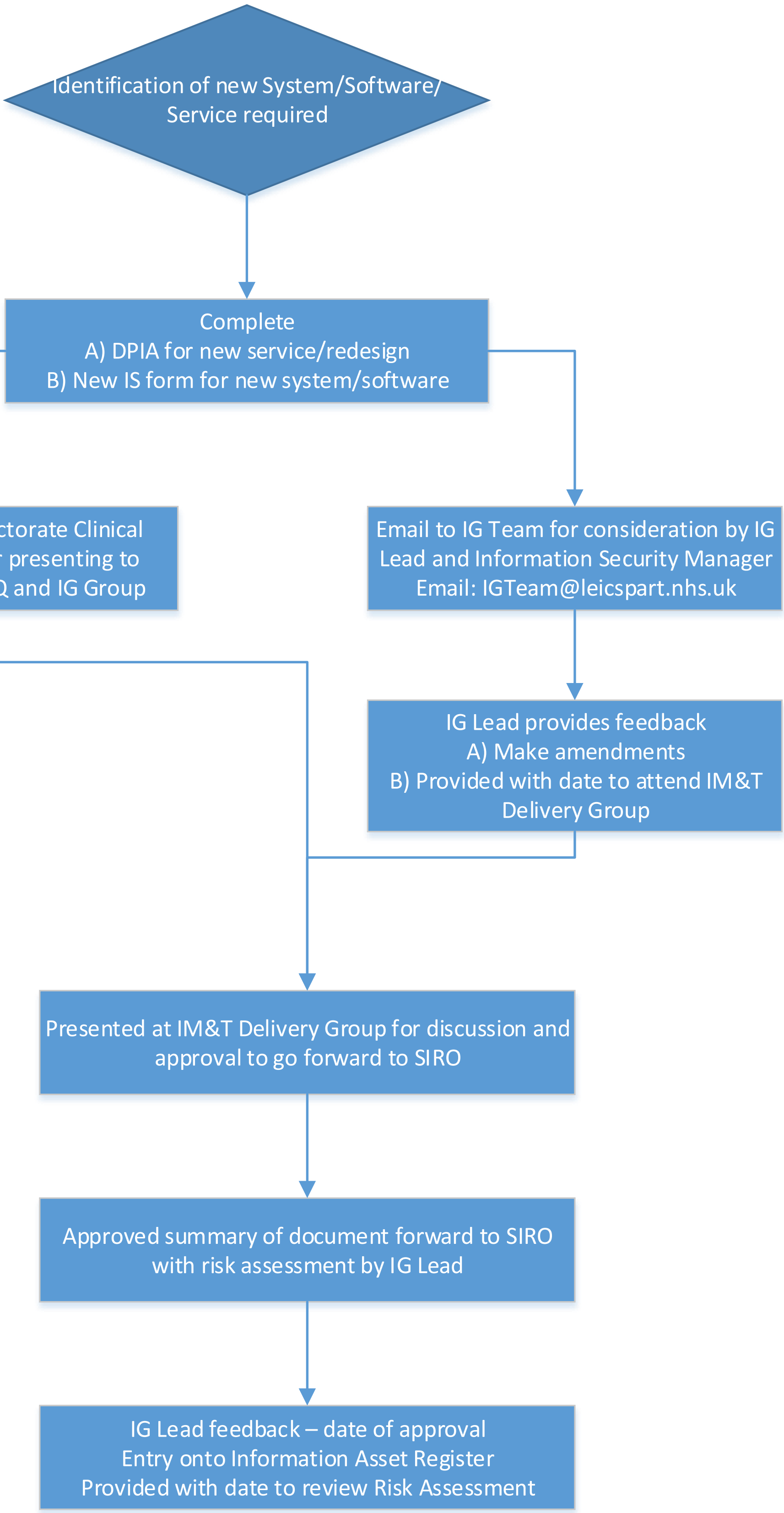
Detailed guidance on the management and definition of roles and responsibilities to information risk within NHS organisations has been prepared by the Department of Health (via NHS Digital) in the policy document NHS Information Risk Management (January 2009). This policy reflects the wider government guidelines set out in the Cabinet Office Report Data Handling Procedures within Government.

The role of the SIRO is to take ownership of the Trust’s information risk policy, to act as an advocate for information risk on the board and provide written advice to the accounting officer on the content of their statement of internal control in regard to information risk.

4.0 Asset Identification and Process Flowchart

Figure 1: Overview of Process


IDENTIFICATIO
N OF ASSET(S)
IAO/IAA
IDENTIFICATIO
N
PIA/PSA
CONTRACTOR
REQUIREMENT
SLSP & RISK
ASSESSMENT
BUSINESS
CONTINUITY
Process
Complete
Asset is
accredited
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 Clinical Directorate Clinical Governance lead for presenting to Directorate IM&T,DQ and IG Group
Email to IG Team for consideration by IG Lead and Information Security Manager
Email: IGTeam@leicspart.nhs.uk
IG Lead 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 IG Lead
IG Lead feedback – date of approval
Entry onto Information Asset Register
Provided with date to review Risk Assessment

5.0 Duties

Senior roles within the organisation supporting the Data Privacy and Security agenda are held by the Organisation’s Senior Information Risk Owner (SIRO), the Caldicott Guardian, the Head of Information Governance; all are supported by the IG Team.

5.1 **Trust Board**

In his communications with NHS Trusts Chief Executives, the NHS Chief Executive has made it clear that ultimate responsibility for aspects of IG in the NHS rests with the Board of each organisation.

5.2 **Chief Executive**

The Trust's Accountable Officer is the Chief Executive who has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risk is handled in a similar manner to other risks such as financial, legal and reputational risks. Reference to the management of information risks and associated information governance practice is required in the Assurance Statement which the Accounting Officer is required to sign annually.

5.3 **Caldicott Guardian**

The Caldicott Guardian also holds the position of Medical Director. The Caldicott Guardian role:

- Is advisory
- Is the conscience of the organisation
- Provides a focal point for patient confidentiality and information sharing issues
- Is concerned with the management of patient information.

The Caldicott Guardian is the person with overall responsibility for protecting personal confidential data (PCD). The Caldicott Guardian plays a key role in ensuring that the organisation and partner organisations abide by the highest level for standards for handling PCD and adherence to the Caldicott Principles.

It is the responsibility of the Caldicott Guardian to feedback any data privacy issues to the Senior Management Team. The Caldicott Guardian is supported by the Head of Information Governance. The Caldicott Guardian chairs the Clinical Effectiveness Group, which receives quarterly Caldicott Reports.

5.4 **SIRO (Senior Information Risk Owner)**

The SIRO is the Chief Nurse/ Deputy Chief Executive. The role:

- Is accountable;
- Fosters a culture for protecting and using data;
- Provides a focal point for managing information risk and incidents
- Is concerned with the management of all information assets.

The SIRO is an executive Board member with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level.

5.5 **Information Asset Owner (IAO) – Clinical Service Directors**

The SIRO is supported by Information Asset Owners who are responsible for the running the services within their Clinical Services. Their role is to understand what information is held, what is added, and what is removed, how information is moved, who has access and why. As a result they are able to understand and address risks to clinical information assets they "own" and to provide assurance to the SIRO on the security and use of the assets.

5.6 **Information Asset Administrators (IAA)**

IAA's work with an information asset on a day to day basis. Within the Trust, this responsibility forms part of the role of Application Support staff within the Leicestershire Health Informatics Service who have day to day responsibility, and key staff within the Clinical Directorate to ensure that policies and procedures are followed by staff and recognise actual or potential security incidents.

5.7 **Information Governance Lead**

The Information Governance (IG) Lead is the Head of Information Governance. The Information Governance Lead is responsible for ensuring the organisation meets is statutory and corporate responsibilities and engender trust from the public in the management of their personal information.

The Head of Information Governance is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG. The key tasks include:

- Responsibility for delivering a high quality specialist Information Governance Service to the Trust;
- To provide strategic direction, planning and guidance to ensure compliance with data privacy and security legislation and the national agenda
- Ensure work practices are evaluated and supported through the development of appropriate policy and procedures across the organisation.
- Acts as Data Protection Officer for the Trust.

5.8 **Information Security Lead**

The LHIS Information Security Manager is responsible for the provision and management of a high quality, customer focussed, Information Technology Security Advisory Service using expertise to manage security issues, identifying best practice and making recommendations for local implementation.

5.9 **All Trust Employees**

All Trust employees and anyone else working for the organisation (eg. Agency staff, honorary contracts, management consultants etc) who use and has access to Trust information must understand their personal responsibilities for information governance and comply with UK Law. All staff must comply with Trust policies, procedures and guidance and attend relevant education and training events in relation to IG.

6.0 Policy

6.1 **Management of Risk**

The Trust operates within an integrated governance framework which aims to ensure that all of the strands of governance such as financial, clinical and non-clinical (including information risk), research and management of risk are coherent. The Trusts management and assurance arrangements rely on on-going risk management processes which identifies risks. Information risks that may result in reputational damage, financial loss, or exposure, major breakdown of information system or information integrity are escalated through the risk management process established as part of the Risk Management Strategy. Staff members are expected to adhere to their contract of employment with the Trust at all times and follow Trust policies and procedures.

The requirement is a positive and robust approach to be taken to managing information risk. The Trust recognises that the purpose of information risk management is not to eliminate all risks relating to information but rather to provide the organisation with the means to identify, prioritise and manage risks in order to provide a balance between the costs of managing and treating risks and the anticipated benefits that may be derived from this action.

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 will base 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 will be allocated to a senior accountable manager. Information asset administrator roles will be allocated to operational staff with day to day responsibility for managing risks within their designated information asset. Administrators will be supported where appropriate by the Health Informatics Service with responsibility for providing technical assistance on information risk management.

Information risk management is a component of information governance but the introduction of a hierarchy of accountability that sits within operational managers and their services rather than within IT services requires a different approach.

The SIRO and IAO’s need to be supported to identify and mitigate information risk. The aim is to ensure that the approach to information risk management:

- Sets out accountability and responsibility structures that are fit for purpose in that they ensure that information risks are managed effectively at all levels in the Trust.

- Associates tasks with appropriate levels in the organisation and in partnership with the Informatics Services;
- Provide transparency in the way in which information risks are managed.

6.2 **Information Asset Management**

The Information Asset Management Process is managed by the Information Security Manager for the Trust. In order to give assurance that an asset is not going to be a major risk for the Trust a process of approval will be developed 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 at section 4.0 gives an overview of how we ensure an asset is 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 Information Security Manager will register the assets on the Information Asset Register; this is the current register for all Trust assets.

Identification of Information Assets and moving forward as a Trust, with the approval process in place will continue 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 Information Governance Lead will liaise with the Information Security Manager 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 / PSA

Data Protection Impact Assessment – a form of risk assessment required for new or changes to systems dealing with personal confidential data. Please see Privacy Impact Assessment Policy and Procedures for further details.

Patient 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 Requirments (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 completed to ensure that all aspects of security are considered.

The SLSP template can be requested from the Information Governance Team via email: IGTeam@leicspart.nhs.uk

A risk assessment is also carried out with links to the information recorded via the SLSP – each aspect of security is considered and if issues arise they are recorded as part of the risk assessment and all are presented to the SIRO to ensure the risks are acceptable risks for the Trust.

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.

6.3 The Process

This process is vital in achieving the strategic aim of the Trust in ensuring data is secure and safe.

Services need to begin preparation in identifying responsibility for service assets as the approval process develops; the Information Security Manager in conjunction with the Information Governance Lead 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.

All new information assets being procured and implemented through the Business Development Team or Clinical Directorate Senior Management Team will be advised through the Clinical Directorate IM&T, DQ and IG Groups to ensure the approval process is complete before forwarding to the IM&T Delivery Group for discussions and final approval of the new Information Asset.

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'.

See Figure 2 at Section 4.0 - Information Asset Approval Process

The process enables information risk to be reduced and active participation is encouraged. If you would like help or support in Asset Management please contact Information Governance: IGTeam@leicspart.nhs.uk

6.4 **Risk Assessments**

Risk assessments will be performed on all information systems and critical information assets owned and operated by the Trust. Risk assessments will be completed for each information asset contained within the asset register by the Information Asset Administrator (IAA). In completing the assessments, the IAA will be supported by the Information Governance Function.

Risk assessments will occur at the following times:

- Annually in preparation for the Assurance Statement to the Chief Executive;
- At the inception of new systems, applications or facilities' that may impact on the assurance of Trust information of systems;
- As a result of any significant changes, enhancements or upgrades to existing critical information systems or applications;
- When NHS policy requires risks to be assessed;
- When the Trust's IM&T Delivery Group, IM&T Strategy Group or Board of Directors requires it.
- When there has been an adverse incident.

The Trust's Records and Information Governance Group will receive information risk report from the Information Security Manager in accordance with its annual work plan.

A report of Information Risks is presented to IM&T Delivery Group, in the form of the IM&T risk register, with specific detail given to the risks that have a risk rating of sixteen (15) or higher. The SIRO will ensure mitigation and effective management of those risks can been seen through marked progress within the reports, where possible.

6.5 **Information Incident Management**

Information incident reporting will be 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:

- Health and Social Care Information Centre;
- The Information Governance Function will provide a quarterly summary of incidents, progress against investigations.

6.6 **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.

6.7 **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 will undertake 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 will undertake 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 will be 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.

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. This is incorporated in the Trust Data Protection and Security Training (formally Information Governance Training). The course directory e-source link below will identify who the training applies to, delivery method, the update frequency, learning outcomes and a list of available dates to access the training.

A record of the event will be recorded on ULearn

The governance group responsible for monitoring the training is Records and Information Governance Group

8.0 Monitoring Compliance and Effectiveness

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
11	Ownership for each asset will be allocated to a senior accountable manager	Section 6.1	Review of Information Asset Register	Records and Information Governance Group	Annually as part of IGT/Data Protection & Security Toolkit Review
12 & 13	Asset Approval process followed	Section 6.2 & Section 6.3	Review of Asset Approvals	Records and Information Governance Group	Annually as part of IGT/Data Protection & Security Toolkit Review
14	Information incident reporting will be in line with the Trust's overall incident management reporting processes	Section 6.5	Incident trends and themes explored through Caldicott Report	Clinical Effectiveness Group Records and Information Governance Group	Quarterly Bi-monthly
15	The Trust will undertake an annual information flow mapping exercise and from this exercise to determine the information risks	Section 6.7	Review of data flows	Records and Information Governance Group	Annually as part of IGT/Data Protection & Security Toolkit Review

9.0 Standards/Performance Indicators

TARGET/STANDARDS	KEY PERFORMANCE INDICATOR
An effectively supported Senior Information Risk Owner takes ownership of the organisation's information risk policy and information risk management strategy	• There is a SIRO with an effective support infrastructure in place and adequate information risk skills, knowledge and experience to successfully co-ordinate and implement information risk management. • The SIRO and supporting Information Risk Management leads (IAOs and

	supporting staff) are appropriately trained and conduct regular risk reviews for all key assets - The arrangements for information risk management are regularly reviewed to ensure they remain current and effective. The SIRO successfully completes strategic information risk management training at least annually

10.0 References and Bibliography

This policy was drafted with reference to the following:

Caldicott (2013) the Information Governance Review

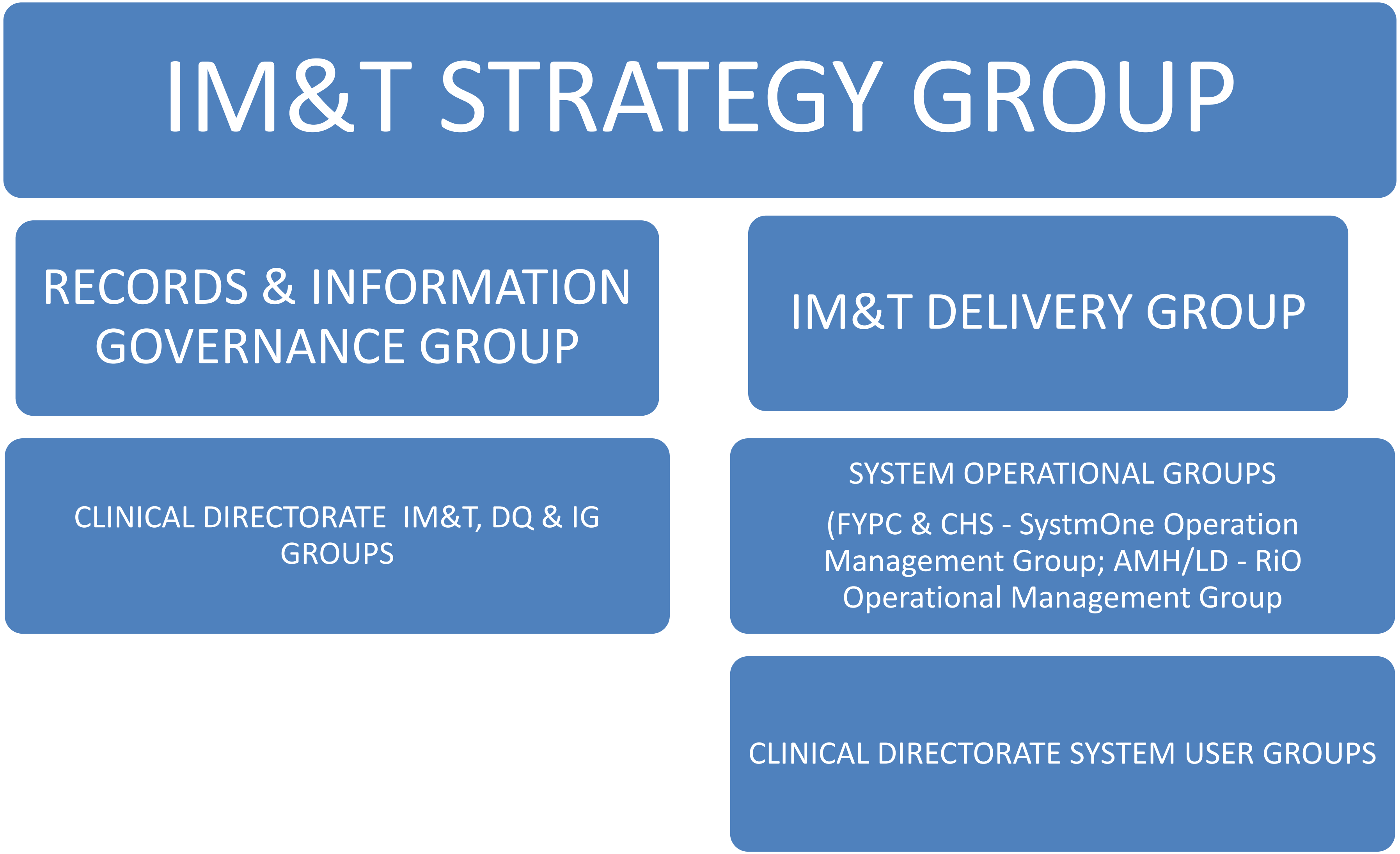
Data Protection Act 1998 http://www.legislation.gov.uk/ukpga/1998/29/contents	The Act provides a legal framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing of information and the Act applies to all forms of media, including paper and images. It applies to confidential patient information but is far wider in its scope, i.e. it covers personnel records. The Data Action principles which regulate the use of patient identifiable data (personal data) are: (i) Fair and lawful (ii) Used only for specified and lawful purposes (iii) Adequate, relevant and not excessive to need (iv) Accurate and kept up to date (v) Not kept for longer than necessary (vi) Processed in accordance with data subject rights, including rights of access (vii) Kept secure and protected against accidental disclosure, loss or damage (viii) Not transferred outside the EEA.
Common Law of Confidentiality	This is not codified in an Act of Parliament but built up from case law where practice has been established by individual judgements. The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Whilst

	judgements have established that confidentiality can be breached in the “public interest” these have centred on case by case considerations of **exceptional** circumstances. Confidentiality can also be overridden or set aside by legislation.
Caldicott Principles	1) Justify the purpose 2) Don’t use patient identifiable information unless it is absolutely necessary 3) Use the minimum necessary patient identifiable information 4) Access to patient identifiable information should be on a strict need to know basis. 5) Everyone should be aware of their responsibilities 6) Understand and comply with the law. 7) The duty to share can be as important as the duty to protect patient confidentiality

Information Governance Policy
Data Protection Impact Assessment Policy and Procedures
Data Privacy, Confidentiality and Caldicott Policy
Information Sharing Policy
The Incident and Serious Untoward Incident and Near Miss Reporting Policy
Information Security Policies

Appendix 1

SIRO Accountability Structure



IM&T STRATEGY GROUP

RECORDS & INFORMATION GOVERNANCE GROUP

IM&T DELIVERY GROUP

CLINICAL DIRECTORATE IM&T, DQ & IG GROUPS

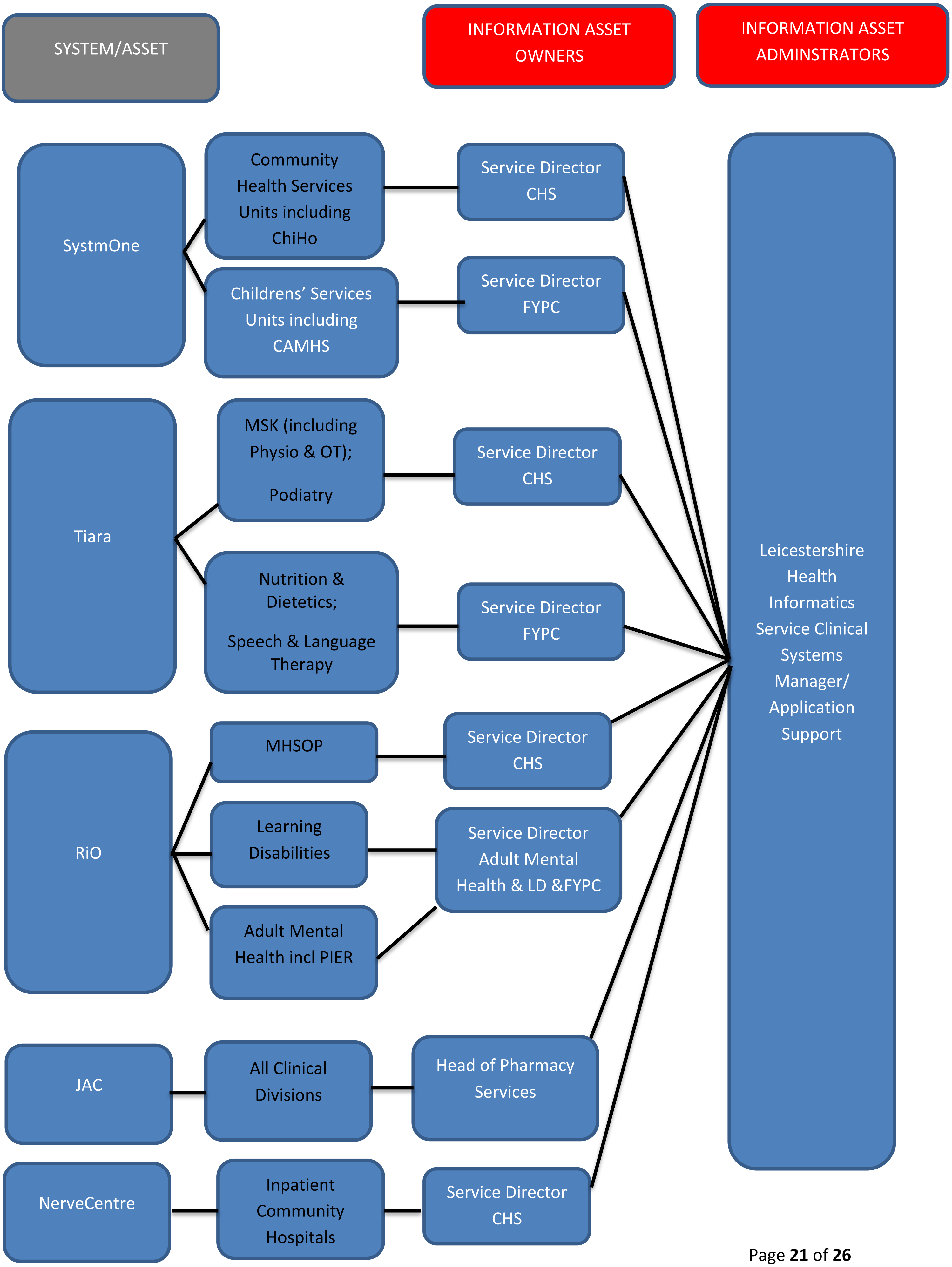
SYSTEM OPERATIONAL GROUPS

(FYPC & CHS - SystmOne Operation Management Group; AMH/LD - RiO Operational Management Group

CLINICAL DIRECTORATE SYSTEM USER GROUPS

Appendix 2

INFORMATION ASSET MANAGEMENT STRUCTURE FOR KEY INFORMATION SYSTEMS (CLINICAL)



SYSTEM/ASSET

INFORMATION ASSET OWNERS

INFORMATION ASSET ADMINSTRATORS

SystmOne

Community Health Services Units including ChiHo

Service Director CHS

Childrens' Services Units including CAMHS

Service Director FYPC

Tiara

MSK (including Physio & OT);

Podiatry

Service Director CHS

Nutrition & Dietetics;

Speech & Language Therapy

Service Director FYPC

RiO

MHSOP

Service Director CHS

Learning Disabilities

Adult Mental Health incl PIER

Service Director Adult Mental Health & LD &FYPC

JAC

All Clinical Divisions

Head of Pharmacy Services

NerveCentre

Inpatient Community Hospitals

Service Director CHS

Leicestershire Health Informatics Service Clinical Systems Manager/ Application Support

Appendix 3

Training Requirements

Training Needs Analysis

Training Required	YES✓	NO
Training topic:	Information Governance	
Type of training: (see study leave policy)	✓ Mandatory (must be on mandatory training register) ☐ Role specific ☐ Personal development	
Division(s) to which the training is applicable:	✓ Adult Mental Health & Learning Disability Services ✓ Community Health Services ✓ Enabling Services ✓ Families Young People Children ✓ Hosted Services	
Staff groups who require the training:	All Staff Groups	
Regularity of Update requirement:	Annually	
Who is responsible for delivery of this training?	Learning and Development via eLearning platform	
Have resources been identified?	Yes	
Has a training plan been agreed?	Yes	
Where will completion of this training be recorded?	✓ ULearn ☐ Other (please specify)	
How is this training going to be monitored?	Monthly training reports to managers	

Appendix 4

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	✓
Support and value its staff	☐
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	✓

Appendix 5

Stakeholders and Consultation

Key individuals involved in developing the document

Name	Designation
Vicky Hill	LHIS Information Security Manager
Mary Stait	Information Governance Compliance Manager

Circulated to the following individuals for comment

Name	Designation
Members of Records & Information Governance Group	
Members of IM&T Delivery Group	

Appendix 6

Due Regard Screening

Section 1	
Name of activity/proposal	Information Risk Policy
Date Screening commenced	October 2017
Directorate / Service carrying out the assessment	Enabling/ Information Governance
Name and role of person undertaking this Due Regard (Equality Analysis)	Sam Kirkland, Head of Information Governance
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The policy lays out the framework for a formal risk management programme explicitly around the accountability and responsibility arrangements for information risk identification, analysis, mitigation and oversight of the process	
OBJECTIVES: The intention is to embed information risk management into the business processes and functions where key assurances are required around the management of information and associated assets	

Section 2	
Protected Characteristic	**If the proposal/s have a positive or negative impact please give brief details**
Age	Positive – the standard of risk management is set out in section 6.1
Disability	Positive – the standard of risk management is set out in section 6.1
Gender reassignment	Positive – the standard of risk management is set out in section 6.1
Marriage & Civil Partnership	Positive – the standard of risk management is set out in section 6.1
Pregnancy & Maternity	Positive – the standard of risk management is set out in section 6.1
Race	Positive – the standard of risk management is set out in section 6.1
Religion and Belief	Positive – the standard of risk management is set out in section 6.1
Sex	Positive – the standard of risk management is set out in section 6.1
Sexual Orientation	Positive – the standard of risk management is set out in section 6.1
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 tick 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 based on nationally recognised standards for the management of Information Risk with an expectation of the identification of risks to service users/patients regardless of any protected characteristics. Sections 6.5 and 6.7 of the policy document outline the considerations given to patients/service users and the information that may be provided.			
Signed by reviewer/assessor		**Date**	October 2017
Sign off that this proposal is low risk and does not require a full Equality Analysis			
Head of Service Signed		**Date**	