INFORMATION RISK POLICY

Unique Reference / Version				
Primary Intranet Location	**Policy Name**	**Version Number**	**Next Review month**	**Next review year**
Information Governance	**Information Risk Policy**	**2.0**	**November**	**2015**

Current Author	Phil Cottis
Author's Job Title	Information Governance & RA Manager
Department	IM&T
Ratifying Committee	Information Governance Committee
Ratified Date	7th November 2013
Review Date	November 2015
Owner	Barbara Cummings
Owner's Job Title	Director of Planning and Performance

It is the responsibility of the staff member accessing this document to ensure that they are always reading the most up to date version. This will always be the version on the intranet

Related Policies	Confidentiality Code of Conduct Data Protection Policy Health Records Management Policy IG framework for projects and system releases, including associated documentation Information Governance Policy Information Security Policy Information Lifecycle and Records Management Policy Safe Haven Procedure

Stakeholders	Information Governance Committee Non Clinical Governance Committee

Version	Date	Author	Author's Job Title	Changes
V1	September 2010	Nic McCullagh	Information Governance Manager	
V2	September 2012	Phil Cottis	IG & RA Manager	Review and new format

Short Description
The purpose of this Information Risk Policy is to protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant.

Key words
Consequence, Information asset owner, Likelihood, Risk Management.

INFORMATION RISK POLICY

CONTENTS

INFORMATION RISK POLICY

1 INTRODUCTION

1.1 The Trust Executive Board has approved the introduction and embedding of information risk management into the key controls and approval processes of all major business processes and functions of the Trust. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and the Trust itself.

1.2 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk. The Board recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

1.3 The Board acknowledges that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls – and not to impose risk management as an extra requirement.

2 PURPOSE

2.1 The purpose of this Information Risk Policy is to:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- Encourage pro-active rather than re-active information risk management
- Provide assistance to and improve the quality of decision making throughout the Trust
- Meet legal or statutory requirements; and
- Assist in safeguarding the Trust's information assets

2.2 This policy is applicable to all areas of the Trust. Adherence should be included in all contracts for outsourced or shared services as responsibility remains with the Trust, even if an agent or subcontractor processes data on our behalf. There are no exclusions.

2.3 For the purpose of this policy, 'staff' is used as a convenience to refer to all staff regardless of occupation, including but not restricted to permanent, fixed-term, contractors, bank , agency, temporary, honorary, visiting, voluntary and students.

3 DEFINITIONS

3.1 Risk

The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood.

3.2 Consequence

The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

3.3 Likelihood

A qualitative description or synonym for probability or frequency.

3.4 Risk Assessment

The overall process of risk analysis and risk evaluation.

3.5 Risk Management

The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

3.6 Risk Treatment

Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:

- Avoid the risk;
- Reduce the likelihood of occurrence;
- Reduce the consequences of occurrence;
- Transfer the risk; and
- Retain/accept the risk.

3.7 Risk Management Process

The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

4 RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive is the accounting officer responsible for the management of the Trust and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to the Trust being able to supply a first class confidential service that provides the highest quality patient care. The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.2 Senior Information Risk Owner (SIRO)

The Trust has appointed the Director of Planning & Performance as Senior Information Risk Owner (SIRO). The SIRO will act as an advocate for information risk on the Board and in internal discussions will provide written advice to the Accountable Officer on the content of their annual Statement of

Internal Control in regard to information risk.

4.3 **Information Asset Owners**

The Information Asset Owners (IAOs) shall ensure that information risk assessments are performed on all information assets where they have been assigned 'ownership', following guidance from the SIRO on assessment method, format, content, and frequency. IAOs shall submit the risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks. The risk assessments for key information assets are to be reviewed annually or as systems are upgraded.

4.4 **Information Governance Committee**

The IG Committee is responsible for ensuring this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

4.5 **Information Governance Team**

The Information Governance Team, with the relevant IAO, will undertake Information Governance Assessments at the planning stage of all new or upgraded systems to ensure compliance to IG and legal requirements. These must be approved by the SIRO before the asset can be implemented.

4.6 **Trust Management**

Directors/Heads of Department/Departmental Managers etc will be responsible for ensuring that staff for whom they are responsible are aware of their responsibilities with regard to confidentiality of information, ensuring that staff receive appropriate confidentiality training.

They will be responsible for ensuring that their staff are fully aware of the mechanisms for reporting actual or potential confidentiality breaches within the Trust.

4.7 **All Staff**

All employees and anyone working on behalf of the Trust must adhere to this policy to support the reputation of the Trust and where relevant of their profession. Employees must make sure that they conduct themselves online in the same manner that would be expected of them in any other situation.

5 RELATED INFORMATION

5.1 It is a core IG objective that all Information Assets of the organisation are identified, that the business importance of those assets is established, that an information risk assessment is undertaken, and that this is recorded on the Trust's Information Asset Register. The Information Asset Owners are responsible for ensuring this is undertaken. The ICT Department maintains the Information Asset Register.

5.2 All new systems and upgrades / releases to existing systems must be risk assessed prior to implementation to identify, prioritise and manage

information risks. This is achieved via the IG framework for projects and system releases, and associated documentation such as the IG checklist which forms part of the risk management process. The new system / upgrade / release must be deemed as compliant and approved by the SIRO prior to implementation.

5.3 Any residual information risks should be recorded, as per any other risk, in the division / departmental risk register and managed as per the Trust's risk management process. Information risks that so warrant it will be recorded on the Trust Risk Register and managed as per the Trust's risk management process.

6 REFERENCES

6.1 References to Standards

- Information Governance Toolkit v.11

7 ARRANGEMENTS FOR MONITORING COMPLIANCE WITH THIS POLICY

Compliance with this policy will be monitored in the following manner (see table below):

Key elements (Minimum Requirements)	Process for Monitoring (e.g. audit)	By Whom (Individual / group /committee)	Frequency of monitoring	Responsible individual / group / committee (plus timescales(for		
				Review of Results	Development of Action Plan	Monitoring of action plan and implementation
Reducing the number of confidentiality breaches	Management of incidents relating to Data Protection	IG Team	Monthly	Information Governance Committee	Relevant Manager according to the issue	Information Governance Committee
Roles and responsibilities	Monitored at appraisal, following review of the individual's knowledge & skills framework (KSF) together with the job description.	Line manager	Annually			
How the organisation provides information risk Training. In house training sessions are delivered regularly throughout the year to meet the needs of the Trust	Electronic Staff Record (ESR) is utilised to identify all staff who are non-compliant	IG Team	Monthly	Information Governance Committee	IG Mandatory Training Working Group	Information Governance Committee
Ensuring best practice across the Trust	Undertaking Confidentiality Audits	IG Team	Monthly	Information Governance Committee	IG Team	Information Governance Committee

APPENDIX 1 EQUALITY IMPACT ASSESSMENT

To be completed and attached to any policy document when submitted to the appropriate committee for ratification

STAGE 1 - SCREENING

Name & Job Title of Assessor: Phil Cottis, Information Governance & RA Manager			**Date of Initial Screening: 24.06.10**
Policy or Function to be assessed: Information Risk Policy			
		Yes/No	**Comments**
1.	**Does the policy, function, service or project affect one group more or less favourably than another on the basis of:**		
	3.1 Race & Ethnic background	No	This policy is applied equally to all groups
	3.2 Gender including transgender	No	This policy is applied equally to all groups
	3.3 Disability:- This will include consideration in terms of impact to persons with learning disabilities, autism or on individuals who may have a cognitive impairment or lack capacity to make decisions about their care	No	This policy is applied equally to all groups
	3.4 Religion or belief	No	This policy is applied equally to all groups
	3.5 Sexual orientation	No	This policy is applied equally to all groups
	3.6 Age	No	This policy is applied equally to all groups
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	This policy is applied equally to all groups

If the answer to any of the questions above is yes, please complete a full Stage 2 Equality Impact Assessment.

Signature of Assessor: Phil Cottis, Information Governance & RA Manager **Date: 07.11.13**

Signature of Line Manager: Barbara Cummings: Director of Planning & Performance **Date: 07.11.13**

APPENDIX 2 PLAN FOR DISSEMINATION OF PROCEDURAL DOCUMENTS

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Acknowledgement: University Hospitals of Leicester NHS Trust

Title of document:	**Information Risk Policy**		
Date finalised:		**Dissemination lead: Print name and contact details**	**Phil Cottis** **IG & RA Manager** **phil.cottis@qehkl.nhs.uk**
Previous document already being used?	**Yes**		
If yes, in what format and where?	**Electronic format on IG Intranet page & Policies & Procedures: Information Governance**		
Proposed action to retrieve out of date copies of the document:	**Remove outdated policy from Trust Intranet**		

To be disseminated to:	**How will it be disseminated, who will do it and when?**	**Format**	**Comments:**
All staff	**IG Intranet page & Policies & Procedures: Information Governance**	**Electronic**	**Trust Staff advised through IG newsletter**

Dissemination Record - to be used once document is approved

Date put on register / library of procedural documents:	**November 2013**	**Date due to be reviewed:**	**November 2015**

Disseminated to: (either directly or via meetings, etc.)	**Format (i.e. paper or electronic)**	**Date Disseminated:**	**No. of Copies Sent:**	**Contact Details / Comments:**
IG Newsletter	Electronic	Jan 2014	1	

APPENDIX 3 CHECKLIST FOR THE REVIEW AND APPROVAL OF PROCEDURAL DOCUMENTS

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	INFORMATION RISK POLICY	
		Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Is the method described in brief?	Yes	
	Are individuals / stakeholders / users involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are local/organisational supporting documents referenced?	Yes	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
	Does the document identify which committee will ratify it?	Yes	
	If appropriate, have the joint Human Resources/staff side committee (or equivalent) approved the document?	NA	
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	**Document Control**		
	Does the document identify where it	Yes	

	Title of document being reviewed:	INFORMATION RISK POLICY	
		Yes/No/ Unsure	Comments
	will be held?		
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	**Process for Monitoring Compliance**		
	Are there measurable standards or KPIs to support monitoring compliance of the document?	Yes	
	Is there a plan to review or audit compliance with the document?	Yes	
10.	**Review Date**		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so, is it acceptable?	Yes	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Phil Cottis	**Date**	30 September 2013
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Barbara Cummings	**Date**	7 November 2013
Signature			

Acknowledgement: Cambridgeshire and Peterborough Mental Health Partnership NHS Trust