The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

INFORMATION RISK POLICY

Primary Intranet Location	Version Number	Next Review Year	Next Review Month
Information Governance	4	2021	September

Current Author	Phil Cottis
Author's Job Title	Head of Health Records & IG
Department	Business Support
Ratifying Committee	Information Governance Committee
Ratified Date	13th September 2018
Owner	Jon Wade
Owner's Job Title	Chief Operating Officer

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	Adverse Events Policy Confidentiality Code of Conduct Data Protection Policy IG Checklist Procedure Information Governance Policy Information Governance Strategy Information Security Policy

Stakeholders	Information Governance Committee Trust Executive Committee

Version	Date	Author	Author's Job Title	Changes
V1	September 2010	Nic McCullagh	Information Governance Manager	New Document
V2	September 2012	Phil Cottis	IG & RA Manager	Review and new format
V3	September 2015	Phil Cottis	IG & RA Manager	Review
V3.1	May 2018	Phil Cottis	Head of Health Records & IG	GDPR compliant
V4	September 2018	Phil Cottis	Head of Health Records & IG	Review. Minor changes

Purpose
The purpose of this policy is to protect the Trust, its staff and its patients from information risk, where the likelihood of occurrence and the consequences are significant. This policy will provide a consistent framework in which information risk will be identified, considered and addressed in key approval, review and control processes.

Key words
Assessment, IAA, IAO, Information Asset, Information Asset Owner, Risk,

CONTENTS

INFORMATION RISK POLICY

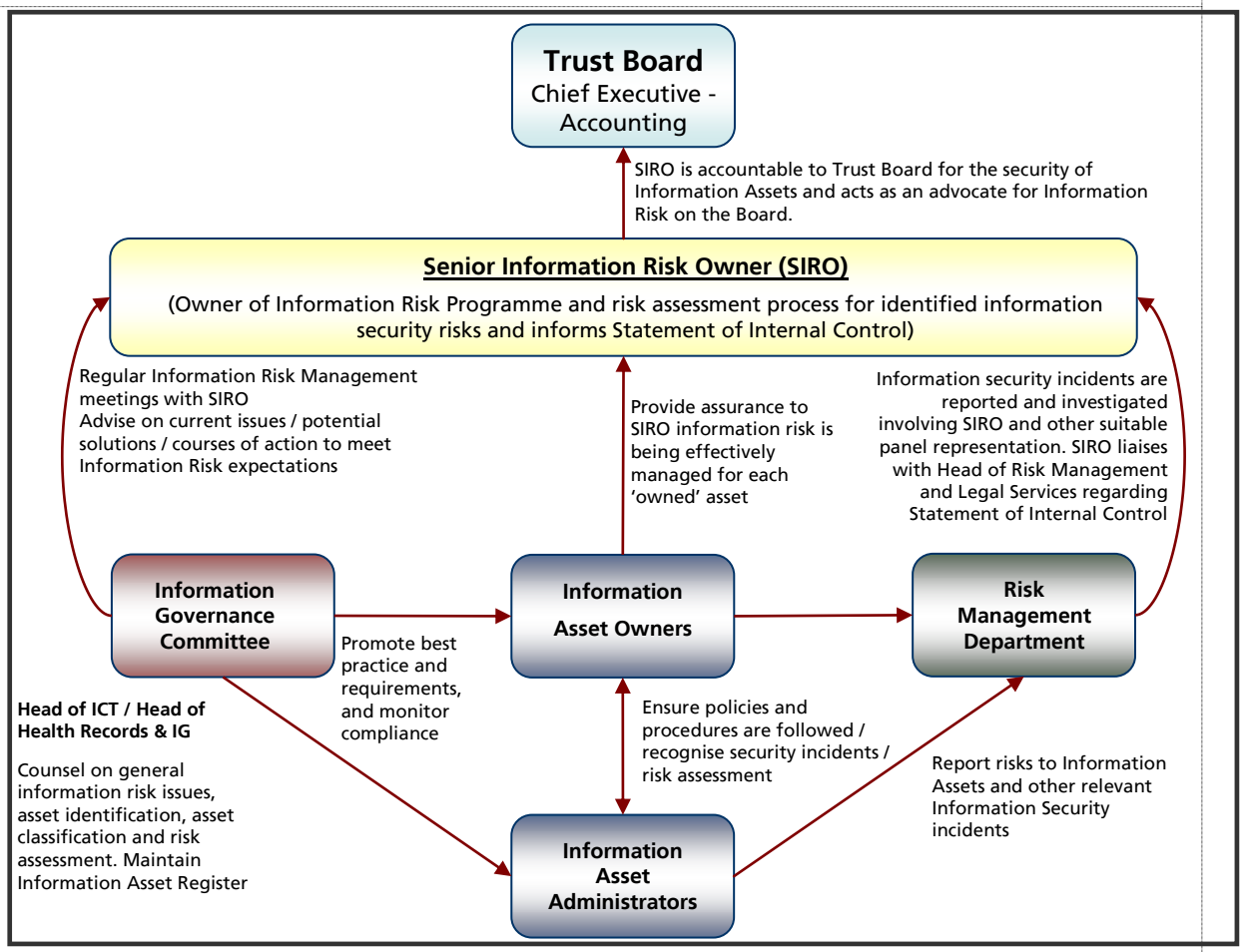
1	**INTRODUCTION**
1.1	The Trust Board has approved the introduction and embedding of information risk management into the key controls and approval processes of all major business processes and functions of the Trust. This decision reflects the high level of importance placed on minimising information 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 Trust 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 Trust 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.
1.4	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.
1.5	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. IPM, 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. IPM, ESR • Audit data • Back up and archive data
Other Information Assets	**System or process documentation**
• Environmental services, e.g. power	• System information and

	and air conditioning • People skills and experience • Shared services, including networks and printers • Server rooms • Training rooms and equipment • Record libraries and archive stores	documentation • Operations and support procedures • Manuals and training materials • Contracts and agreements • Business continuity and disaster recovery plans
2	**PURPOSE**	
2.1	The purpose of this policy is to protect the Trust, its staff and its patients from information risk, where the likelihood of occurrence and the consequences are significant. This policy will provide a consistent framework in which information risk will be identified, considered and addressed in key approval, review and control processes.	
2.2	This will encourage proactive risk management, provide assistance to, and improve the quality of, decision making throughout the Trust and help to safeguard the Trust's information assets.	
2.3	This policy is applicable to all areas of the Trust and adherence should be included in all contracts for outsourced or shared services.	
2.4	Whilst the Risk Management Strategy and associated risk management policies are applicable to all risks, this policy identifies those additional measures which are specific to the management of information risks.	
3	**DEFINITIONS**	
3.1	**Consequence** Consequence is the outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, disadvantage or gain. There may be a range of possible outcomes associated with an event.	
3.2	**Information Assets** In general Information Assets will be administration systems or database used to process PID directly or used in any way that has the potential to affect the confidentiality / integrity / availability / legal processing of PID. The following outlines the main examples of Information Assets: • Databases and data files; • System information and documentation; • Back-up and archive data; • Operations and support procedures; • Audit data; • Applications and system software; • Data encryption utilities; • Development and maintenance tools; • Paper records (including patient care notes and staff records); • Environmental services necessary for the safe operational of Information Assets (e.g. power and air conditioning); and • Business continuity plans.	

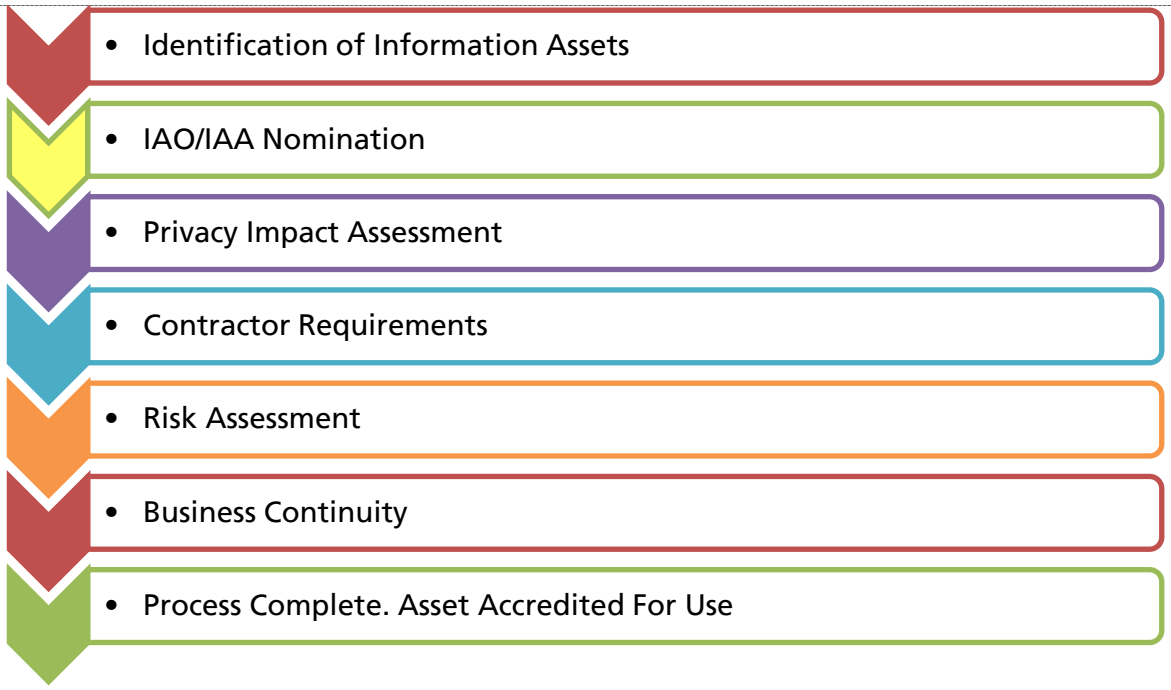
3.3	**Information Asset Owners** Information Asset Owners (IAOs) are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'. Information Asset Owners may be assigned ownership of several assets of their organisation.
3.4	**Information Asset Administrators** Information Asset Administrators (IAAs) are usually operational members of staff who understand and are familiar with information risks in their area or department.
3.5	**Information Asset Register** Information Asset Register (IAR) is the mechanism by which an organisation records the Information Assets that it holds. The existence of which is a requirement of the Information Governance Toolkit.
3.6	**Information Risk** Information Risk is a risk that relates to the loss, damage, or misuse of information or which threatens the confidentiality, integrity or availability of an information asset, especially information which is personal or confidential in nature.
3.7	**Likelihood** Likelihood is a qualitative description for probability or frequency.
3.8	**Personal Confidential Data (PCD)** Personal confidential data relates to information about a person which would enable that person's identity to be established by one means or another. This might include: • Name, address, post code, date of birth; • Pictures, photographs, videos, audio-tapes or other images of patients; • NHS number and local patient identifiable codes; and • Anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
3.9	**Risk Assessment** Risk Assessment is the overall process of risk analysis and risk evaluation.
3.10	**Risk Management** Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives, whether positive or negative) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.
3.11	**Risk Register** The Trust uses a Risk Register to consistently record risks that it has identified.
3.12	**Risk Treatment** Risk Treatment is the selection and implementation of appropriate options for dealing with risk which, conceptually, will involve one or a combination of the

	following strategies: • Risk avoidance; • Reduction in the likelihood of occurrence; • Reduction in the consequences of occurrence; • Risk transference; and • Risk tolerance / acceptance.
4	**RESPONSIBILITIES**
4.1	**Chief Executive** The Chief Executive is the Accounting Officer and has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level, where information risks are handled in a similar manner to other major risks such as financial, legal and reputational risks.
4.2	**Senior Information Risk Owner (SIRO)** The SIRO acts as an advocate for information risk on the Board and in internal discussions will provide written advice to the Accounting 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) are senior individuals involved in running the relevant business / service areas. The IAO role is to: • Understand and address risks to the information assets they 'own'; and • Provide assurance to the SIRO on the security and use of these assets.
4.4	**Information Asset Administrators** Information Asset Administrators (IAAs) provide support to their IAO. To do this they will: • Ensure that policies and procedures are followed; • Recognise potential or actual security incidents; • Consult their IAO on incident management; and • Ensure that information asset registers are accurate and maintained and kept up-to-date.
4.5	**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.
4.6	**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.
4.7	**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.
4.8	**All Staff** All staff should be aware of information risk management, how to raise risks and incidents, and have responsibility for ensuring that information is kept secure. Secure practices can help: • Avoid unauthorised disclosure, dissemination or access to information; and • Support appropriate storage, transportation, transfer and disposal of information.
5	**INFORMATION RISK MODEL**
5.1	
5.2	**Aims**
5.2.1	The aim of information risk management 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 proactive rather than reactive 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.
5.2.2	The key requirement is for information risk to be managed in a robust way within work areas and not to be seen as something that is the sole responsibility of ICT or Information Governance staff. Assurance needs to be provided in a consistent manner. To achieve this, a structured approach is needed, building upon the existing Information Governance Management Framework. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff (Information Asset Owners).
5.2.3	Information Asset Owners (IAOs) are supported by Information Asset Administrators (IAAs), who are operational staff with day-to-day responsibility for managing risks to their information assets. The IAOs are responsible for ensuring information risk is managed appropriately and for providing assurance to the SIRO.
5.2.4	The aim is to ensure that the approach to risk management: • Takes full advantage of existing authority and responsibility structures where these are fit for purpose; • Associates tasks with appropriate management levels; • Avoids unnecessary impacts on day to day business; and • Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner.
5.3	**Management Lead**
5.3.1	Managers must acknowledge that information is valuable and risks must be mitigated. They must portray the importance of handling information through their decisions and actions. • All staff should know good information handling as part of their job; • Senior staff will understand they are bound by the same rules as junior staff. They must not override, for reasons of convenience, risk controls; • All staff should be able to answer general questions about information protection and make sensible information risk decisions for themselves, including knowing the limits of their competence and when to defer to others for guidance; • All staff personal development plans should include competencies on information handling; • It is the responsibility of the Trust Board to ensure that the Trust has an open approach to incidents and learning; and • The Trust Board must encourage staff to question instructions that seem inappropriate on information risk grounds and must encourage reporting on instances of inappropriate behaviour.
5.4	**Information Risk Management Programme**
5.4.1	An information risk management programme must be aligned to the Trust Business

	Plan to support individual objectives and ensure they are adequately resourced. The information risk management programme should cover: • The balance between level of risk, tolerance of risk and the effort being used to manage the risk; • Identification of gaps between the current and target risk positions; • Progress being made against agreed information risk priorities; and • The effectiveness of the risk management controls including successes and failures.
5.5	**Information Risk Mitigation**
5.5.1	Information risk mitigation must: • Be commensurate with the level of risk – it does need to remove the risk entirely; • Be kept simple so that it is manageable and can be communicated to staff; • Include monitoring and reporting on the on-going level of information governance / confidentiality / information security breaches, so that the effectiveness of the protection being achieved can be assessed; • Risk must be assessed in terms of the general level of harm that could be reasonably caused if data were to become compromised or unavailable; • Take the form of a wide range of controls directed at reducing the likelihood of an information (confidentiality, integrity or availability) failure and reduce the amount of harm a failure could cause; • Control and reduce the likelihood and amount of harm of a failure and enhance overall mitigation; • Apply 'good practice' controls, which are easy for staff to understand and apply; and • Be supplemented with customised controls for specific high risk circumstances.
6	**INFORMATION ASSET MANAGEMENT**
6.1	The Information Asset Management Process is managed by the Information Governance Team within the Trust. In order to give assurance that an is not going to be a major risk for the Trust a process of accreditation has been 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.
6.2	The process below gives an overview of how we ensure an asset is accredited for use:



6.3	**Identification of Assets**
6.3.1	The first stage in the process is the identification of all existing assets and the need for them to be accredited for use. The ICT team will maintain the Information Asset Register.
6.3.2	Identification of Information Assets and moving forward as a Trust with the accreditation process with 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.
6.4	**IAO / IAA Identification**
6.4.1	When an asset needs a review of its accreditation or a new asset is to be accredited the Information Governance Team will assign a lead to help with the process. The first stage is the identification of responsibility and assigning an Information Asset Owner and Information Asset Administrator.
6.5	**Data Protection Impact Assessment(DPIA)**
6.5.1	A DPIA is a form of risk assessment required for new or changes to systems/information assets dealing with personal identifiable / sensitive data. DPIA's are undertaken by the Information Governance Team and are informed through the IG Checklist process.
6.6	**Contractor Requirements**
6.6.1	It is essential to ensure that when an asset is accredited for use that the correct checks are carried out to reduce the risk to the Trust by ensuring the contractor is fit for purpose and can meet statutory and regulatory standards.

6.7	**Service Level Security Policy (SLSP) and Risk Assessment**
6.7.1	In order to further reduce and / or be able to manage risk within the accreditation process a System Level Security Policy is completed to ensure that all aspects of security are considered.
6.7.2	A risk assessment is also carried out, by each IAO/IAA, 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 for the Trust.
6.8	**Business Continuity**
6.8.1	Each IAO / IAA is required to provide a Business Continuity Plan which also helps the accreditation process to mitigate risks within the Trust. The Trust can then be confident that a service has thought about service provision if a system becomes unavailable.
7	**THE PROCESS**
7.1	**Overview**
7.1.1	This process is vital in achieving the strategic aim of the Trust in ensuring data is secure and safe.
7.1.2	Services need to begin preparation in identifying responsibility for service assets as the accreditation process is now developing; the Information Governance Team is developing a programme of accreditation and will be contacting services to assist and support the process of ensuring assets already in situ within the Trust become accredited for use.
7.1.3	All new information assets are being procured and implemented through the ICT Team which links directly with the IG department to ensure the accreditation process is complete before final implementation of the new Information Asset.
7.1.4	The process is followed and all information is analysed and assessed for risks that need to be brought to the attention of the Senior Information Risk Officer (SIRO). The SIRO is presented with the information at the IG Committee and he assesses the information and 'signs the information asset of' as 'accredited for use'.
7.1.5	Information Asset Management Training is available to provide in depth training on the process and practical help on completing the documents; this training is recommended.
7.1.6	The process enables information risk to be reduced and active participation is encouraged. If you would like help or support in Information Asset Management please contact Information Governance at IGHelp@qehkl.nhs.uk
7.2	**Risk Assessments**
7.2.1	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 information asset register by the IAO/IAA). IAOs/IAAs will be supported by the IG Team complete the risk assessments.
7.2.2	Risk assessments will occur at the following times: • Annually in preparation for the statement of internal control 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; and • When there has been an adverse incident.
7.2.3	A report of Information Risks is to be presented to the IG Committee bi-monthly with specific detail given to the risks that have a risk rating of sixteen (16) or higher. The SIRO is to ensure mitigation and effective management of those risks can been seen through marked progress within the reports, where possible.
7.2.4	Periodically an internal audit will be undertaken in relation to information risks in order to assess the effectiveness of the risk assessments and risk management plans.
7.3	**Information Incident Management**
7.3.1	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 & Management Policy.
7.4	**Information for the Public**
7.4.1	The Trust will promote transparency about its information risk and incidents. An information charter will be published setting out how it handles information and will set out in its Annual Report and Statement of Internal Control summary material on information risks. This will include the number of incidents and serious untoward incidents, number of people potentially affected and action was taken to contain the breach and prevent recurrence. The Trust will conduct privacy impact assessments as part of its information governance improvement plan.
7.4.2	The Trust will consider where appropriate, notifying patients when an actual or suspected breach has taken place in line with legislation and guidance from the Information Governance Review.
7.5	**Adoption of Specific Action to Protect Patient Information**
7.5.1	The Trust places significant importance on the need to protect personal confidential data (PCD) particularly where release or loss may result in harm or distress to the individuals concerned.
7.5.2	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.
7.5.3	The Trust will undertake periodic information flow mapping reviews to determine the information risks regarding its data flows within the organisation and with its partners.
7.5.4	The Trust will undertake to minimise the risk from unauthorised access to PCD. This includes holding and accessing data on ICT 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.
8	**TRAINING**
8.1	All staff (including agency staff, locums and volunteers) within the Trust will be required to undertake mandatory Induction training on information governance issues, including security and confidentiality.
8.2	In addition, staff will also be required to undertake mandatory annual refresher information governance training.
8.3	Additional training on aspects of information risk management and assessment will be provided to the SIRO, IAOs and IAAs and the Caldicott Guardian.
8.4	Performance in managing information risk will be reflected in staff management processes. Failure to comply with Trust policy and procedures relating to the protection of information security and confidentiality may lead to disciplinary action.
9	**EQUALITY IMPACT ASSESSMENT**
9.1	A Stage 1 (Screening) - Equality Impact Assessment has been undertaken and no negative impact on any group was indicated (see Appendix 1).
10	**REFERENCES**
10.1	**References to Standards** • Data Security and Protection Toolkit v.15
10.2	**Legislation** • Common Law Duty of Confidentiality • Data Protection Act (2018) • EU General Data Protection Regulation
10.3	**Guidance** • Ensuring Security and Confidentiality in NHS Organisations (E5498) • NHS Confidentiality Code of Practice (November 2003)

11 MONITORING COMPLIANCE

11.1 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
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 IG 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
Reducing the number of Information Governance breaches	Management of incidents relating to Information Governance	IG Team	Monthly
Risk assess all information assets	Audit the number of information risk assessments	IG Team	Monthly
Ensuring best practice across the Trust	Undertaking Confidentiality Audits	IG Team	Monthly

APPENDIX 1

EQUALITY IMPACT ASSESSMENT
Equality Impact Assessment Tool
(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 – IG & 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:**		
	• Race & Ethnic background	No	
	• Gender including transgender	No	
	• 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	
	• Religion or belief	No	
	• Sexual orientation	No	
	• Age	No	
2.	**Does the public have a perception/concern regarding the potential for discrimination?**	No	

Signature of Assessor: Phil Cottis **Date: 17th August 2018**
Head of Health Records & IG

Signature of Line Manager: Jon Wade **Date: 13th August 2018**
Chief Operating Officer