Joint Policy for Cumbria Partnership Foundation Trust & North Cumbria University Hospital NHS Trust

Information Risk Policy (Joint)

Reference	POL/IG/014
Version	1.0
Date Ratified	28/05/2019
Next Review Date	May 2022
Date Published	29/05/2019
Accountable Director	Director of Finance, Digital and Estates
Policy Author	IG Compliance Manager

Please note that the Intranet / internet Policy web page version of this document is the only version that is maintained.

Any printed copies or copies held on any other web page should therefore be viewed as "uncontrolled" and as such, may not necessarily contain the latest updates and amendments.

Policy On A Page

SUMMARY & AIM

This policy is for identifying the actions required to be taken, and the accountability and responsibility arrangements, for information risk identification and management.
This is to ensure compliance with relevant standards and legislation.

The aim of the policy is:

To outline both Trusts approach to risk management and to have a single integrated approach.
Staff must always adhere to this policy in relation to risk management.

TARGET AUDIENCE:

This policy applies to all staff and services within the Cumbria Partnership NHS Foundation Trust (CPFT) and North Cumbria University Hospitals Trust (NCUH), including private contractors, Volunteers, temporary staff and is applicable to any organisation under contract with IG services.

TRAINING:

Appointed Information Asset Owners and SIRO need to be accredited to fulfil this role by completing a workbook. See section on training for specifics for all levels of staff.

KEY REQUIREMENTS

All staff (permanent, temporary, agency etc.) who use and have access to Trust information must understand their personal responsibilities for information governance and comply with UK Law.

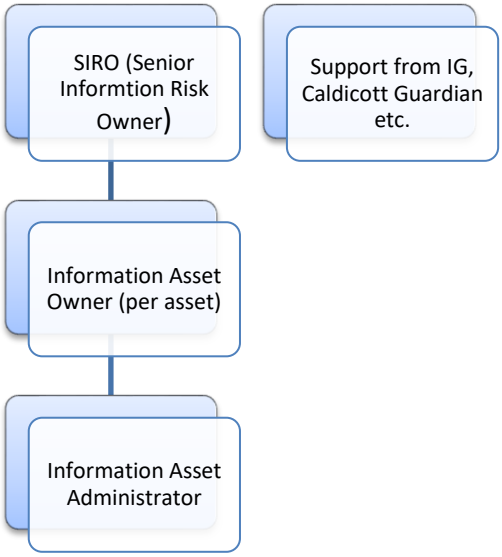
All staff must comply with Trust policies, procedures and guidance and complete relevant IG education and training.

All staff to understand the portfolio of responsibilities under Information Governance and request assistance and support at appropriate times on a case by case basis.

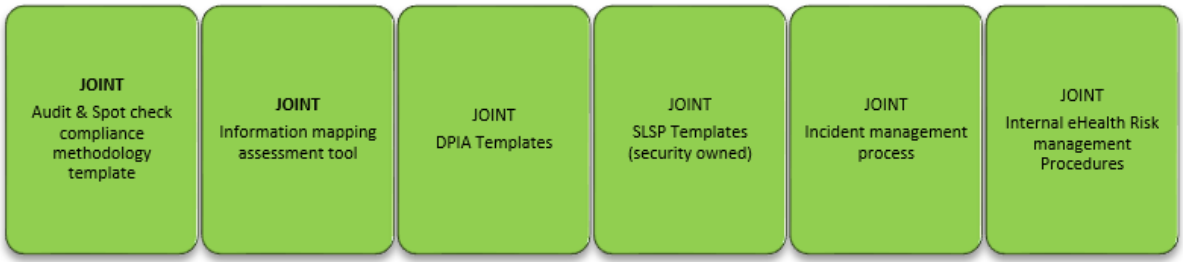
TABLE OF CONTENTS

SUMMARY FLOWCHART:

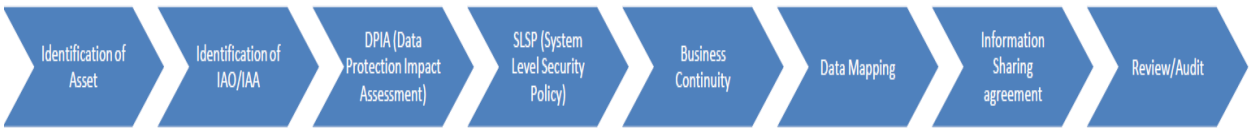
Information Asset Owner Structure



INFORMATION RISK TOOLS



INFORMATION ASSET MANAGEMENT STAGES



1. INTRODUCTION

This policy sets out the risk management mechanism for Cumbria Partnership NHS Foundation Trust (CPFT), and North Cumbria University Hospitals NHS Trust (NCUHT) and North Cumbria Clinical Commissioning Group (NCCCG) to achieving a secure information handling and management structure within the organisations. Information is an invaluable resource to CPFT and NCUHT and its loss can damage their reputation, service delivery, and its misuse can damage the organisations and individuals.

CPFT and NCUH have a legal obligation to comply with all appropriate legislation in respect of data, information and IT security. It also has a duty to comply with guidance issued by the Department of Health, Information Commissioner's Office, NHS Digital and other advisory groups and professional bodies that provide guidance to staff.

The Policy lays the framework for a formal Information Risk Management programme in the Trusts by explicitly establishing the accountability and responsibility arrangements for risk identification and analysis, planning for information risk, mitigation, and the oversight of Information Risk Management.

This document should be read in conjunction with all Trust information governance, risk and information security policies which are available on the intranet.

2. PURPOSE

The Trusts have a commitment to ensure that information risk is managed in accordance with all relevant regulations and guidance. The purpose of this Policy is to formally establish the Trusts' 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 Trusts' strategic business objectives and should enable staff across the organisations to identify an acceptable level of risk beyond which escalation of risk management decisions is necessary.

Specific information risk processes:

- Define how the Trusts and its partners will manage information risk and how risk management effectiveness will be assessed and measured
- Protect the Trusts from those information risks of significant likelihood and consequence which may impact on its ability to deliver its stated strategic aims and objectives
- Provide a consistent framework through which information risks relating to business processes and functions within the Trusts 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 Trusts' information assets which comprise of, but are not limited to, people, finance, property and reputation.

  Information risk is inherent in all Trust activities.

3. POLICY DETAIL

3.1 The Trust will not accept information risks that may result in damage to reputation, financial loss or exposure, major breakdown of information system or information integrity, significant incidents of regulatory non-compliance, potential injury to staff, patients or their family or carers or other people working on behalf of the trust. Failure to comply with Trust policy and procedures relating to the protection of information security and confidentiality may lead to disciplinary action.

3.2 A positive and robust approach is to be taken to managing information risk. The Trusts recognise that the purpose of Information Risk Management is not to eliminate all risk 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.

3.3 Information risk is the responsibility of all staff. Staff have a responsibility to protect the security of confidential information particularly when it is person identifiable information. All staff should therefore actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate action.

3.4 A structured approach is required 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.

The Information Asset Management Process is managed by the IG Compliance Team within the Trusts. In order to give assurance that an asset 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 Trusts we are ensuring the highest level of security and mitigating risk as much as is possible.

All information systems and equipment where data is held will be recorded on the IM&T Asset register ("Information Asset Store"). Ownership for each asset will be allocated to a senior accountable manager or clinician, the Information Asset Owner (IAO). Information Asset Administrator (IAA) roles will be allocated to operational staff with day to day responsibility for managing risks within their designated information asset.

An Information Asset Register is a mechanism for understanding and managing an organisation's assets and the risks to them – including the links between the information assets, their business requirements and technical dependencies. It is a requirement for the Data Security and Protection Toolkit that a record of all

Information Assets that the Trusts hold, together with details on the Information Asset Owner and Administrator is held within an Information Asset Register.

3.5 IAOs should familiarise themselves with the risk management practices of their organisations, specifically how to identify, understand, manage, report and record risks. Understanding your organisation's risk appetite is also important, as it will help you to align any risk-based decisions you make regarding assets for which you are responsible, with the wider organisational approach.

An IAO's role is a key element in an organisation's efforts to manage information risk. SIROs will look to IAOs for the day to day management of information risk and to highlight systematic risks which the organisation may need to address. The IG department follow the Trusts' scoring rationale.

For your purposes risk appetite can be defined as: a threshold set by your organisation, relating to the level of risk it considers acceptable and which should not be exceeded, unless approved by your SIRO.

3.6 Risk assessments will be performed on all information systems and critical information assets owned and operated by the Trusts. Risk assessments will be completed for each information asset contained within the asset register by the Information Asset Owner (IAO). In completing the assessments the IAOs will be supported by Information Asset Administrators (IAAs) and the technical specialists in the IM&T Directorate.

Risk assessments will occur at the following times:

- Annually for the review of information risk for the SIRO to support the SIRO's written advice on 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

A Data Protection Impact Assessment (DPIA) should be carried out whenever a new process or information asset is likely to involve a new use or significantly change the way in which personal Identifiable information is handled.

3.7 The development, implementation and management of a SLSP will help to demonstrate understanding of information governance risks and commitment to address the security and confidentiality needs of a particular system.

It will also help to ensure that information security standards and processes are in place across the Trust that meet the requirements of the Information Governance Toolkit and align with ISO/IEC 27001:2013.

The SLSP shall be the responsibility of the Information Asset Owner (IAO), who shall be responsible for its content and regular review. Tasks can be delegated to the Information Asset Administrator (IAA).

3.8 Information incident reporting will be generally in line with the Trusts' overall Incident Reporting Policy and Procedure. The Trusts will promote transparency about its information risks and incidents and will set out in its Annual Report a summary on information risks. This will include the number of incidents and serious untoward incidents, number of people potentially affected and action taken to contain the breach and prevent recurrence.

3.9 The Trusts will use data handling clauses from the Crown Commercial Service's 'Frameworks' for services contained within nationally defined forms of contract as its generic information governance model contract for contracts with third parties.

3.10 The Trust places significant importance on the need to protect Person Identifiable Information, particularly where release or loss may result in harm or distress to the individuals concerned.

3.11 The Trust will therefore identify information risk and manage in a secure way the transfer of data to and from other organisations where release or loss could result in a breach of security which could lead to 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 one or all of the categories;

- Any information that links one or more identified or identifiable natural person with information about them where the release would put them at significant risk, harm or distress. This includes all types of special category/sensitive personal information.
- Any information where a person's identity may be inferred from the data items.

3.12 The Information Governance department will periodically undertake a Record of Processing Activity (ROPA) and information mapping/flow exercise. The Trust has a legal responsibility under the General Data Protection Regulations to record all processing activities.
It is a legal responsibility of an organisation to ensure that transfers of personal information for which they are responsible (Data Controller) are secure at all stages and therefore as an outcome of this process technical and organisational measures can be put in place to secure these transfers.

The Information Sharing Gateway provides a tool for IG professionals to work electronically with the ability to register recipient organisations and provides a level of assurance against their compliance (i.e. data and security protection toolkit, PSN etc.). It also signs the organisations up to common information sharing agreement framework.
The Gateway allows data mapping to take place capturing the frequency of data transfer and why, when and, how it's being transferred. This enables a risk

assessment rating so that as Data Controller we can confirm that flows are lawfully and fairly processed.
This information sharing gateway provides details on where flows of data are coming from (i.e. which information asset) and complements the work being done on information asset management. Any information sharing agreements in place should be signed and logged on the portal.

3.13 The Trust will minimise the risk of unauthorised access to protectively marked information. 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. The Trust ensures that all portable computers are encrypted to NHS standards. It ensures the secure destruction and disposal of electronic and paper media through a clearly defined destruction policy and set of procedures which include shredding, confidential waste removal, onsite erasure, degaussing and destruction.

3.14 Action will be taken to minimise the risks presented by unauthorised access to protected 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.

3.15 Compliance spot checks will be undertaken on a monthly basis within a specific area to ensure staff and the work area comply with data protection standards. The spot check is to ensure that the organisation can demonstrate compliance and reduce risk to Trust information, and provide assurance to our patients / clients / staff that their information is being used lawfully and is held securely. The audits will also provide sufficient assurance for the Trust's Senior Information Risk Owner (SIRO) and good quality evidence for the Data Security and Protection Toolkit

3.16 The IG Compliance team will undertake yearly reviews of any critical assets and three yearly reviews on any other asset.

The IG Compliance team will conduct regular audits and spot checks on the Trusts' assets to ensure compliance. The IG Compliance team use the ICO Guide to Data Protection Audits as a guide.

The focus of the audit approach will be to determine whether the organisation policies and procedures are being followed operationally with staff in order to reinforce and educate, regulate the processing of personal data; also to ensure that processing is carried out in accordance with such policies and procedures. When an organisation complies with its requirements, it is effectively identifying and controlling risks to prevent breaching the DPA/GDPR.

An audit will typically assess the organisation's procedures, systems, records and activities in order to:

- ensure the appropriate policies and procedures are in place

- verify that those policies and procedures are being followed
- test the adequacy controls in place
- detect breaches or potential breaches of compliance; and
- recommend any indicated changes in control, policy and procedure.

4. TRAINING AND SUPPORT

Information Governance training is mandatory (set by the Department of Health) for all staff on induction and on a yearly basis. The Information Governance Team will work with the Training Department(s) and managers to ensure that appropriate additional training is available to support staff.

The Information Governance team will work the Senior Information Risk Owner, Information Asset Owners and other appropriate managers and teams to maintain continued awareness of confidentiality and security issues to both the organisation and staff through staff emails, newsletters, intranet etc.

4.1 SIRO, IAO and IAA Training

Information Asset training is compulsory for the SIRO, Information Asset Owners and Information Asset Administrators - this is to be completed every three years.

The training for the SIRO, IAO and IAA will be more in depth and relevant to their role, including risk management training. The training is in the form of a PowerPoint presentation and an assessment.

4.2 Monitoring compliance with this policy

The table below outlines the Trusts' monitoring arrangements for this policy/ document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect of compliance or effectiveness being monitored	**Monitoring method**	**Individual responsible for the monitoring**	**Frequency of the monitoring activity**	**Group / committee which will receive the findings / monitoring report**	**Group / committee / individual responsible for ensuring that the actions are completed**
Initial review of all information assets and annual review of information assets following the introduction of	Quarterly Report	Information Asset Officer	Quarterly	IG Board	Senior Information Risk Owner (SIRO)

the new system.					
Risk Report	Quarterly Report	Head of Information Governance	Monthly	IG Board	Senior Information Risk Owner (SIRO)
Quality check on assets to comply with policy	Audit Methodology	IG Compliance Manager	Annually	Performance Group	Head of IG
Information Governance Training	Training will be monitored in line with the Learning and Development Policy.				
SIRO and IAO Training	Training will be the NHS Digital Training Tool modules: NHS Information Risk Management for SIROs and IAOs, NHS Information Risk Management and Secure Transfers of Personal Data.				

5. PROCESS FOR MONITORING COMPLIANCE

The process for monitoring compliance with the effectiveness of this policy is as follows:

Aspect being monitored	Monitoring Methodology	Reporting		
		Presented by	Committee	Frequency
IM&T Risk Register	Details of IM&T risk	Head of IG	Performance Group	Monthly
Risk action report	Updates on actions taken to treat known risks	Head of IG	Performance Group	Monthly
Audit	Audits of practice in relation information governance and information security risk undertaken as part of the data security and protection toolkit (DSPT)	Head of IG	IG Board	Every 2 months

Wherever the above monitoring has identified deficiencies, the following must be in place:

- Action Plan
- Risks to be included in risk registers
- Progress of action plan monitored at IG Board

6. REFERENCES/BIBLIOGRAPHY:

The Data Security and Protection Toolkit
General Data Protection Regulation 2016
Data Protection Act 2018
Freedom of Information Act 2000
Access to Health Records Act 1990
Human Rights Act 1998
Information Security Management – ISO 27001
The Common Law Duty of Confidentiality
The Caldicott Principles
Records Management: NHS Code of Practice
Information Security Management: NHS Code of Practice
Confidentiality: NHS Code of Practice

7. ASSOCIATED DOCUMENTATION:

Related Trust Policy/Procedures

- Information Governance Strategic Management Framework

For all related IG policies see the IG section on the policy page.

8. DUTIES (ROLES & RESPONSIBILITIES):

Senior roles within the organisation supporting the Information Asset Management process are held by the organisation's Senior Information Risk Owners (SIRO), the Caldicott Guardians, the Head of Information Governance; all are supported by the IG Compliance Team.

8.1 Chief Executive / Trust Board Responsibilities:

The Chief Executive and Trust Board jointly have overall responsibility for the strategic and operational management of the Trust, including ensuring that Trust policies comply with all legal, statutory and good practice requirements.

8.2 Executive Director Responsibilities:

All policies have a designated Executive Director and it is their responsibility to be involved in the development and sign off of the policies, this should ensure that Trust policies meet statutory legislation and guidance where appropriate. They must

ensure the policies are kept up to date by the relevant author and approved at the appropriate committee.

8.3 Accountable Officer

The Trusts' Accountable Officer is the Chief Executive who has overall accountability and responsibility for Information Governance. The Accounting Officer is required to provide assurance, through the Statement of Internal Controls, that all risks to the organisation, including those relating to information, are effectively managed and mitigated to an acceptable level. The Accounting Officer is required to sign the Statement of Internal Control annually.

8.4 Senior Information Risk Owner (SIRO)

This procedure has been written for the purpose of both Cumbria Partnership NHS Foundation Trust and North Cumbria University Hospitals. Statutorily each organisation will require a designated SIRO and hence a different reporting route for relevant queries attributable to this process until full integration can occur. For CPFT the SIRO is the Director of Finance, Strategy and Support Services and for NCUH, the Director of Finance.

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. The SIRO takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the board and provides written advice to the accounting officer on the content of their statement of internal control in regard to information risk. The Information Governance Toolkit defines that every organisation must have a SIRO.

The role of the SIRO:

- Is accountable for approving all Information Assets.
- 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.
- To provide a focal point for the resolution and/or discussion of information risk issue.
- Ensure that all care systems information assets have an assigned Information Asset Owner.
- Ensuring the Organisation has a plan to achieve and monitor the right Information Governance culture, across the organisation and with its business partners.
- Approval of all information asset business continuity plans.
- Document a plan for information security assurance that identifies the support necessary to ensure work related to information security management is appropriately carried out.
- Oversee the development of an Information Risk Policy, and a Strategy for implementing the policy within the existing Information Governance Framework.
- Review and agree action in respect of identified information risks.

8.5 Caldicott Guardian

The Caldicott Guardian(s) ensure both Trusts satisfy the highest practical standards for handling patient-identifiable information. Acting as the '*conscience'* of the organisation, the Caldicott Guardian actively supports work to facilitate and enable information sharing where it is appropriate to share, and advise on options for lawful and ethical processing of information as required.

The Caldicott Guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. This role is particularly important in relation to the implementation of national systems.

8.6 Information Asset Owners (IAO)

The IAOs must ensure that any information asset they are responsible for are properly protected and their value to the organisation is fully recognised. The IAOs have the responsibility for day to day management of the information risk for their asset. 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. The IAO provides an understanding of what information they hold, how important it is, how sensitive it is, how accurate it is, how reliant they are on it, and who's responsible for it. The IAO of Information Assets should be linked to a post, rather than a named individual, to ensure that responsibilities for the asset are passed on, should the individual leave the organisation or change jobs within it.

The role of the IAO is to:

- Be directly accountable to their SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets.
- Ensure their team and those interacting with the asset understand information security and are confident in their handling of information.
- Lead and foster a culture that values, protects and uses information for public good.
- Know who has access and why, and ensure that their use of the asset is monitored.
- Understand and address risks to the asset, provide assurance to the SIRO and ensure any data loss incidents are reported and appropriately managed.
- Ensure any new information assets have a completed data privacy impact assessment and are entered on the Information Asset Register.
- Any changes to an information asset are documented on the Information Asset Register and follow the correct change control process.
- Put procedures and controls in place to ensure the integrity and availability of their information assets.
- Put in place a business continuity plan for any key information assets.

- Are aware of what information is held, and the nature of and justification for information flows to and from the assets for which they are responsible.
- Ensure there is good understanding of the hardware and software composition of their assigned assets to ensure their continuing operational effectiveness. This includes establishing and maintaining asset records that will help predict when asset configuration changes may be necessary.
- Assign Information Asset Administrators (IAA) to their information assets.
- Review their information assets on an annual basis at a minimum.
- To provide a report on the status of the asset to the IG Board on yearly basis.

8.7 Information Asset Administrators (IAA)

The IAAs work with an information asset on a day to day basis. They have day to day responsibility, ensure that policies and procedures are followed by staff and recognise actual or potential security incidents, and consult their IAO on incident management.

The role of the IAA is to:

- Understand and be familiar with information risks in their area or department
- Implement the organisation's information risk policy and risk assessment process for those information assets they support and will provide assurance reports to the relevant Information Asset Owner as necessary
- Ensure the data quality of their Information Asset and report areas of concern to the IAO
- Ensuring that personal information is not unlawfully exploited, under the direction of the IAO
- Recognising potential or actual security incidents and consult the IAO
- Under the direction of their IAO, ensuring that information is securely destroyed when there is no further requirement for it
- Ensuring compliance with data sharing agreements within the local area
- Ensuring that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO
- Reporting to the relevant IAO on current state of local information handling.

8.8 Data Protection Officer

The DPO is a protected and independent role, as the General Data Protection Regulation itself states: "The controller and process shall ensure that the Data Protection does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his / her tasks. The Data Protection Officer shall directly report to the highest level of management of the controller or the processor." In conjunction with the allowance the DPO role can be fulfilled on a basis of a service contract and is permitted a high degree of autonomy to pursue their duties. The DPO primary tasks are outlined in Article 39:

- Inform and advise the controller (Trust) or the data processor (i.e. contractor) and the employees who carry out the processing of their obligations pursuant to this regulation and to other union or member state data protection provisions.
- Monitor compliance with the General Data Protection Regulation including assignment of responsibilities, awareness raising and training of staff involved in processing operations and the related audits.
- Provide advice where requested as regards the Data Protection Impact Assessments and monitor its performance pursuant to article 35.
- To co-operate with the supervisory authority (Information Commissioner) and to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36 and to consult where appropriate, with regard to any other matter.

The Head of Information Governance is the designated Data Protection Officer and Data Privacy Officer and is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Information Governance.

8.9 Information Governance Compliance Team

The Information Governance Compliance team are responsible for providing support and guidance to staff with regard to the management of their Information Assets. The Compliance team will:

- Promote information asset awareness throughout the Trusts by organising training, awareness campaigns and providing written procedures/guidance that are widely disseminated and available to staff.
- Assist with investigations into breaches of confidentiality or data loss of personal and sensitive information.
- Co-ordinate the notifications of such breaches with the Information Commissioner's Office (ICO) and our commissioners.
- Work with the IAO to help mitigate risks to their information assets.

8.10 Registration Authority

The team are responsible for the registration process by which users of Smartcard-enabled IT applications are authenticated (proving who they say they are beyond reasonable doubt) and authorised (enabled to have particular levels of access to particular patient data).

The Registration Authority is the governance framework within which the Trust can register individuals as users to access the NHS Smartcard enabled system(s) - maintaining the confidentiality and security of patient information at all times.
The Registration Authority use a common and rigorous approach to how users are registered and are given access to the national and other services, is an integral part of protecting the confidentiality and security of every patient's personal and health care details.

8.11 Applications

The Applications team are responsible for the implementation and administration, to some extent, of all applications. The Applications team will be consulted with to check the details within the accreditation documents to ensure they are accurate, within the scope of their expertise.

8.12 Data Controller

The Controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

8.13 Data Processor

The processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

8.14 All Trust Employees

All Trust employees and anyone else working for the organisation (e.g. agency staff, honorary contracts, management consultants etc.) who use and have access to Trust information and/or ICT Systems must understand their personal responsibilities for information asset management. All staff must comply with Trust policies and are responsible for Information Security and the correct use of the Information Asset.
Staff must be aware that confidentiality and security of information includes all information relating to patients, service users, carers and employees. Such information may relate to staff or patient/client's records, electronic databases or methods of communication containing personal identifiable information. Staff will be expected to:

- Adhere to the Data Protection Act Policy and any associated procedure and/or guidelines.
- Attend all mandatory training and awareness programmes.
- Ensure that all personal identifiable information is accurate, relevant, and up-to-date and used appropriately on both electronic and manual records and devices.
- Share information on a 'need to know' basis only.
- Ensure that all personal identifiable information is kept safe and secure at all times.
- Ensure they report any incidents and or events that could have an impact on the information asset.

8.15 Approving Committee Responsibilities:

The Chair of the approving committee will ensure the policy approval is documented in the final section of the Checklist for Policy Changes. The committee will agree

the approval of the final draft of the policy. The Joint IG Board is the responsible Committee

9. ABBREVIATIONS / DEFINITION OF TERMS USED

Keep lists in alphabetical order

ABBREVIATION	DEFINITION
	No abbreviations used.

TERM USED	DEFINITION
Asset	An asset can be a single significant document or a set of related data, documents or files; it can be shared or be confined to a specified purpose or organisational unit. It will have recognisable and manageable value, risk, content and lifecycle. The Trusts have hundreds of such systems, both electronic and paper that hold information relating to service users and staff. To assess whether a body of information should be considered an information asset the questions below should be asked: • Does the information have a value to the organisation? • Does the group of information have a specific content? • Does the information have a manageable lifecycle? • Is there a risk associated with the information? • Does the information have a purpose? • Does the information have a disposal schedule?
An information asset	An information asset can be defined as a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively (for examples see appendix 1). The Data Security & Protection Toolkit categorises an information asset as: • Information: Databases, system documents and procedures, archive media/data, paper records etc. • Software: Application programs, system, development tools and utilities. • Physical: Infrastructure, equipment and accommodation used for data processing. • Services: Computing and communications used for data processing.
Critical Information Asset	A critical information asset is one which the organisation is reliant on and cannot operate without. The result of the

TERM USED	DEFINITION
	information asset being unavailable for up to 24 hours will disrupt and have an effect on patient care, quality of service and the operations of the organisation. All critical assets must have a Data Protection Impact Assessment (DPIA), System Level Security Policy (SLSP) and Business Continuity Plan (BCP) in place.
Project/Process:	A system of work or a project that requires an assessment of IG implications but is not in the above two categories. e.g. Operational request for contractor

DOCUMENT CONTROL

Equality Impact Assessment Date	
Sub-Committee & Approval Date	*Joint IG Board 17 May 2019*

History of previous published versions of this document:

Version	Ratified Date	Review Date	Date Published	Disposal Date
N/A				

Statement of changes made from previous version

Version	Date	Section & Description of change
4 2	26/02/2016 24/01/2018	Policy drafted as a result of the integration agenda which merges: • NCUH Information Risk Policy IG18 • Joint Information Asset Management policy POL/IG/004

List of Stakeholders who have reviewed the document

Name	Job Title	Date
IG Board membership	All board members	May 2019
IG Teams both NCUH and CPFT	Various	Feb 2019