NHS
Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE SERVICE BASED POLICY

POLICY AND PROCEDURE FOR INFORMATION GOVERNANCE & INFORMATION RISK

Policy Number:	**IT12**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint SIRO and Information Governance Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**August 2018**
Next Review Date (by):	**August 2021**
Version Number:	**August 2018 – V8**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Information Governance Manager**

TRUST-WIDE SERVICE BASED POLICY POLICY

August 2018 – Version 8

Striving for perfect care for the people we serve

Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE SERVICE BASED POLICY

POLICY AND PROCEDURE FOR INFORMATION GOVERNANCE & INFORMATION RISK

Further information about this document:

Document name	**Policy and Procedure for Information Governance & Information Risk (IT12)**
Document summary	This Policy is issued as a framework to support Information Governance. This document is presented in a standard structure and format. It will be made available in appropriate, alternative languages and formats on request.
Author(s) Contact(s) for further information about this document	**Linda Yell,** **Information Governance Manager** **Telephone: 0151 471 2686** **Email: linda.yell@merseycare.nhs.uk**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **V7 Building** **King Business Park** **Prescot** **Liverpool** **L34 1PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IT02** IM&T Security Policy **IT10** Confidentiality and Information Sharing Policy **IT14** Data Protection Act Policy **IT13** Freedom of Information Policy **IT04** Corporate Records Management Policy **IT06** Corporate Health Records Policy
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Version 1	Approved by Policy Group	March 2010
Version 2	Approved by Policy Group	May 2011
Version 3	Approved by Policy Group	June 2012
Version 4	Approved by Policy Group	December 2013
Version 5	Approved by Information Governance Committee	28 August 2015
Version 6	Approved by Policy Group	17 April 2017
Version 7	Approved by Policy Group	January 2018
Version 8	Approved by Policy Group	August 2018

SUPPORTING STATEMENTS – this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child/adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

CONTENTS

1. EXECUTIVE SUMMARY

1.2 This policy defines the framework to ensure the Trust meets its obligations in relation Information Governance and Information Risk.

1.3 Implementation of and adherence to this policy will ensure:

- Information is held, used and obtained in accordance with the Data Protection Act 2018, European Directive: General Data Protection Regulation and Freedom of Information Act 2000.
- Information is safeguarded against the risk of data breach, loss, damage, destruction.
- Information is used in accordance with NHS Digital and NHS Code of Practice on Confidentiality
- Information is stored in accordance with the NHS Code of Records Management.
- Staff are trained and aware of their responsibilities in respect of Information Governance and Confidentiality.
- This policy is applicable to all staff working for, or with, Mersey Care NHS Foundation Trust who work with either Organisational or Personal identifiable information.

1.4 This policy should be read in conjunction with the following Trust policies:-

- IT02 IM&T Security Policy
- IT10 Confidentiality and Information Sharing Policy
- IT14 Data Protection Act Policy (General Data Protection Regulation)
- IT13 Freedom of Information Policy
- IT04 Corporate Records Management Policy
- IT06 Corporate Health Records Policy

2. INTRODUCTION

2.1 RATIONALE

2.1.1 Mersey Care NHS Foundation Trust recognises the importance of information, both in the terms of the clinical management of individual service users and the efficient management of services and resources. Information Governance policies play a key part in supporting Clinical Governance, service planning and performance management. Adherence to robust policies also gives assurance that information is dealt with legally, securely, efficiently and effectively, in order to meet legal and good practice responsibilities.

2.1.2 The Trust Board has also 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 service users, staff and the Trust itself.

2.1.3 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.

2.1.4 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.

2.1.5 The Executive Director - Finance, is the nominated Senior Information Risk Owner (SIRO) for the Trust and the Medical Director is the nominated Caldicott Guardian for the Trust. The Information Governance Manager is the lead for Information Governance and the Data Protection Officer within the Trust.

2.2 SCOPE

2.2.1 This policy applies to all staff, volunteers and contractors who undertake any activity within the organisation.

2.2.2 This policy covers all aspects of information use and information risk management within the organisation, including but not limited to:-

- Patient/Service user information
- Personnel information
- Organisational Information
- Information Assets

2.2.3 The policy covers all aspects of handling information including, but not limited to:-

- Structured record systems-paper and electronic
- Transmission of information - fax, email, post and telephone.

2.2.4 This policy covers all information systems purchased, designed, developed and managed on the behalf of, the organisation and any individual directly employed or otherwise by the Trust.

2.2.5 The Trust's Information Governance Committee has overall responsibility for overseeing the implementation of the Information Governance framework and is accountable to the Executive Committee, who will in turn ensure that Information Governance and Information Risk Management is embedded within the organisation structure. The Trust's Joint Senior Information Risk Owner and Information Governance Committee has 'day to day' operational responsibility to promote and implement compliance with the Information Governance framework.

2.3 PRINCIPLES

2.3.1 Information Governance ensures that one of the Trusts most important assets, information, in both clinical and management terms, is respected and held in a secure and manageable conditions. It is therefore of paramount importance to ensure that information is efficiently managed on the basis of the HORUS categorization:

- Held safely and confidentially
- Obtained fairly and effectively
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

2.3.2 The Trust has put into place a range of appropriate policies, procedures and management arrangements to provide a robust framework for Information Governance. It will maintain polices and procedures to ensure compliance with the requirements of the Data Security and Protection Toolkit.

3. POLICY

3.1 The Information Governance Policy has been developed to provide a robust assurance framework that the Trust will work within to meet current legislation. The Information Governance (IG) agenda is driven by Department of Health (DoH) policy that, itself, is derived from a need to comply with obligations imposed by key 'data handling' legislation. These are, primarily, the Data Protection Act 2018, European Directive: General Data Protection Regulation and Freedom of Information Act 2000 but include other relevant legislation. These statutory obligations are supplemented by further DoH/NHS policy recommendations that define the scope of the IG agenda and all obligations placed on NHS Trusts by it. This policy is driven by a recognised need to handle both personal and corporate information in an appropriate manner

through the creation and maintenance of an internal Information Governance framework. A suitably robust IG framework will:-

- Contribute to the delivery of compliance, as defined
- Ensure all aspects of information quality in the delivery of healthcare services to local citizens, and
- The appropriate use of corporate data for Trust purposes.
- Protect the Trust, its staff and its patients/service users from information risk, where the likelihood of occurrence and the consequences are significant.
- 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.

3.2 Annual completion of the Data Security and Protection Toolkit is the 'backbone' of evidence provided by the Trust which enables measurement of current data handling standards and any improvements made to them, year on year.

4. IMPLEMENTATION

4.1 There are 4 key interlinked strands to the Information Governance Agenda.

- Openness
- Legal Compliance
- Information Security
- Quality Assurance

4.2 Openness

4.2.1 The Trust recognises the need for an appropriate balance between openness, its duty of candour and confidentiality in the management of information and its uses.

4.2.2 Information will be identified and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations and principles as outlined in the Data Protection Act 2018, European Directive: General Data Protection Regulation. Non-confidential information held by the Trust will be available to the public through a variety of means to ensure compliance with the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

4.2.3 Patients/service users have access to information relating to their own healthcare, options for treatment and their rights as patients/service users. There are clear policies, procedures and arrangements for handling queries from patients and the public. The Trust Privacy Notice contains further information in respect of the processing and sharing of information with other organisations.

4.2.4 The Trust has clear procedures and arrangements for liaison with the press and broadcasting media.

4.2.5 Requirements of all information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

4.2.6 Availability of information for operational purposes will be maintained within set parameters relating to its importance.

4.2.7 The Trust will ensure that the exchange/sharing of any information is only carried out when necessary, within the scope of the Trust's Information Commissioner's Office Registration and within strict guidelines under which information was obtained and outlined at the time or with the person's consent.

4.2.8 The Trust has established and maintains policies and procedures to ensure compliance with the Data Protection Act 2018, European Directive: General Data Protection Regulation , Human Rights Act, the common law duty of Confidentiality and the Freedom of Information Act.

4.2.9 Training in Information Governance will be provided to all staff upon Induction and thereafter on an annual basis to ensure that staff are aware of their responsibilities. All volunteers, contractors, bank staff will also be required to complete Information Governance training.

4.2.10 Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine that appropriate, effective and affordable information governance controls are in place.

4.3 Legal Compliance

4.3.1 Mersey Care NHS Foundation Trust is obliged to comply with all relevant UK and European Union legislation. Policies assume that the requirement to comply will be devolved to employees and agents of the Trust guided by policies and standard operating procedures who may be held personally accountable for any breaches of security for which they may be held responsible.

4.3.2 The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements and/or provide the information to undergo these assessments of compliance.

4.3.3 The Trust regards all identifiable personal information relating to service users and staff as confidential, except when law dictates otherwise.

4.3.4 The Trust has established and maintains policies to ensure compliance with the Data Protection Act 2018, EU Directive: General Data Protection Regulation, Human Rights Act and the common law Duty of Confidentiality.

4.4.4 The Trust has established and maintains policies for the controlled appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act and the Crime and Disorder Act, Children Act, etc.)

4.4 Information Security

4.4.1 The Trust has established and maintains policies for the effective and secure management of its information assets and resources.

4.4.2 Audits are undertaken or commissioned to assess information and Information Technology security arrangements.

4.4.3 The Trust promotes effective confidentiality and security practice to all its staff through policies, procedures, audit trail functionality and on-going training.

4.4.4 The Trust will adhere to a clear desk and screen policy, where by all desks will be clear of any working documents or print outs at the end of the working day, and no Visual Display Unit screen will be left unattended at anytime displaying data – automatic system "time-out" application must be in place for systems that are capable of displaying any personal identifiable information.

4.4.5 The Trust requires its staff to ensure that all sensitive, personal and critical data is locked away when not in use – passwords must not be shared by staff or written down and left on display within areas which could lead to unauthorised access to systems.

4.4.6 Network screen warnings should be in place at network system log-on to remind staff of their responsibilities and that audit functionality is in place and monitoring will be undertaken.

4.4.7 The Trust's incident reporting system is used to report, monitor and investigate all breaches or potential breaches of confidentiality and security. All suspected breaches of confidentiality or data loss must be reported as per the Trust Adverse Incident reporting policy.

4.4.8 Any adverse incidents relating to data loss/data breach incidents that meet the Information Commissioners Office reporting criteria will be reported within 72 hours (real time) from the incident notification to comply with the Data Protection Act 2018, EU Directive General Data Protection Regulation.

4.4.9 Review of incidents will be undertaken at the Joint Senior Information Risk Owner Information Governance Committee meeting chaired by the SIRO. The Executive Committee will be provided with bi-monthly IG Chair's reports for assurance purposes. Each Division will receive regular reports in order to investigate issues, identify trends and minimise risk and in turn provide an incident investigation report back to the SIRO and Information Governance Committee

4.5 Information Risk Management

4.5.1 *Whilst the Risk Management Strategy (SA02) and associated risk management policies are applicable to all risks, this policy also identifies those additional measures which are specific to the management of information risks.*

4.5.2 Definitions associated with risk management

4.5.2.1 **Risk** – the chance of something happening, which would have an impact upon objectives. It is measured in terms of *likelihood* and *severity*

4.5.2.2 **Risk Management Process** – the systematic application of management policies, procedures and practices to the task of establishing the context and identifying, analysing, evaluating, treating, monitoring and communicating risk.

4.5.2.3 **Consequence** – 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.

4.5.2.4 **Information Risk** – 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. This includes cyber security incidents.

4.5.2.5 **Likelihood** – a qualitative description for probability or frequency.

4.5.2.6 **Risk Assessment** – the overall process of risk analysis and risk evaluation.

4.5.2.7 **Risk Management** – the culture, processes and structures directed towards the effective management of potential opportunities and adverse effects. 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
- Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner

4.5.2.8 **Risk Treatment** – 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
- Risk tolerance / acceptance

4.5.2.9 **Information Assets** – in general Information Assets will be administration systems or database used to process Personal Identifiable Data (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 and staff records)
- Environmental services necessary for the safe operational of Information Assets (e.g. power and air conditioning)
- Business continuity plans

4.5.2.10 **Information Governance Compliance Framework**
An Information Governance compliance monitoring and management tool is available for review on line.

4.5.2.11 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
- Assist in safeguarding the Trust's information assets

4.5.2.12 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 Compliance Framework. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff (Information Asset Owners).

4.5.2.13 **Information Asset Owners (IAOs)** are designated Senior Managers responsible for ensuring that 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'
- provide assurance to the SIRO on the security and use of these assets
- complete the NHS Digital Data Security Awareness Training module annually
- attend bespoke training for Information Asset Owners.

4.5.2.14 **Information Asset Administrators (IAAs)** are operational staff with day-to-day responsibility for managing risks to their information assets. The IAAs are responsible for ensuring information risk is managed appropriately and for providing assurance to the Information Asset Owners and Senior Information Risk Owner.

4.5.2.15 To do this they will:

- ensure that policies and procedures are followed
- recognise potential or actual security incidents
- consult the IAO and SIRO on incident management
- ensure that information asset registers are accurate and maintained and kept up-to-date
- complete annual Data Security Awareness training.

4.5.2.16 **Management Lead**

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
- All staff must undertake Information Governance Training upon Induction and then on an annual basis.
- 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
- 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

4.5.2.17 **Information Risk Management Programme**

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
- The effectiveness of the risk management controls including successes and failures

4.5.2.18 Information Risk Mitigation

Information risk mitigation must:

- Be commensurate with the level of risk – it does not 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
- Be supplemented with customised controls for specific high risk circumstances

4.5.2.19 Information Incidents

All incidents that constitute an actual or potential loss of information, which could potentially lead to a breach of confidentiality, are to be reported directly to the Patient Safety Team. All such incidents must be documented on an Adverse Incident Form, and could involve:-

- Loss or breach of Service User information
- Loss or breach of staff information
- Loss or breach of confidential business information
- Loss of hardware:
- Laptops
- iPads
- mobile phones
- Virus attacks
- Unauthorised access to systems / information assets
- Misuse of systems / privileges
- Cyber security incidents

4.5.2.19.1 Each incident must be reported within 72 hours (real time) of an incident occurring, these will be reviewed by the Information Governance Manager to assess whether they meet the Information Commissioner's Office reporting criteria and are formally reported via the Data Security & Protection Toolkit to the Information Commissioner's Office.

4.5.2.19.2 The Information Governance Manager will advise the area on the immediate controls that need to be implemented to mitigate the risk of reoccurrence and incident management.

4.5.2.19.3 The Information Governance Manager will notify the Senior Information Risk Owner and Caldicott Guardian to ensure that they are aware of incident and

that the Trust complies with its duty of candour to advise any service users, employees or third party organisation's whose personal data has been breached. This will be either be by formal letter signed by the Senior Information Risk Owner or Caldicott Guardian or by discussion with the service user's clinical team who will undertake the decision when the service user is medically well enough to be informed of the data breach incident and a record of this will be recorded within the service user's clinical record.

4.5.2.19.4 All incidents reported to the Information Commissioner's Office will have a full Root, Cause Analysis investigation undertaken, the investigation report will be overseen by the SIRO, Caldicott Guardian and Information Governance Committee in order ensure that full assurance in risk mitigation is identified

4.5.2.19.5 Information Asset Register Maintenance
Information Asset Owners responsible for overseeing the completion and regular review and update of their Information Asset Registers. Amendments and updates are more likely to be made by Information Asset Administrators, who will have more of an operational and day-to-day knowledge of the Information Assets.

4.5.2.19.6 Information Risk Assurance Reports
Information Asset Owners must provide an annual assurance report to the SIRO on the risk status of their Information Assets and any other areas of information risk considered appropriate. The SIRO will report quarterly to the Integrated Governance Committee on Information Risk Management, which will include the status of risks to information assets.

4.5.2.19.7 Introducing New Information Assets
When new Information Assets are being considered for procurement the Trust must follow its formal due diligence processes. These will be triggered through submission of business cases and approved by the Digital Board – a full Data Privacy Impact Assessment must be completed if the asset collects any element of personal identifiable data and in addition an Information Security Risk Assessment checklist must be completed to ensure that it meets the Trust security standards to enable the asset to be lodged onto the Trust Information Asset Register – the template for the Data Privacy Impact Assessment is attached to this policy – please see Appendix A

4.6 Information Quality Assurance

4.6.1 The Trust has a policy for Data Quality and Records Management policy to ensure the effective management of records. Audits will be undertaken or commissioned to assess the quality of data and record management agreements. Senior Managers within Divisions will be expected to take ownership of, and seek to improve, the quality of data within their services. Wherever possible, information quality will be assured at the point of collection. The Trust promotes data quality and record management through policies, Procedures/user manuals and training, in accordance with national standards.

4.7 Training

4.7.1 All staff will be required as part of Trust Induction to complete the Mandatory Data Security Awareness module or to provide proof that this has been completed at another organisation. This training will be completed annually for existing staff and monitoring will be undertaken by the Joint Senior Information Risk Owner & IG Committee

4.8 Year on Year Improvement Plan and Assessment

4.8.1 NHS Digital requires the Trust to annually assess their performance in Information Governance against the Data Security & Protection Toolkit. Reports and proposed action/development plans will be presented to the Joint Senior Information Risk Owner/IG Committee and the Trust's Executive Committee for approval as a result of the annual Data Security & Protection Toolkit report.

5. MONITORING & COMPLIANCE

5.1 Compliance of this policy will be by the Information Governance Lead ensuring the Trust completion and submission of the Annual Information Governance Toolkit. Compliance against the standards provides the Trust with assurance that a robust framework is in place. Internal monitoring and review will be undertaken by the Joint SIRO and Information Governance Committee with regular provision of a bi-monthly IG Chair's report submitted to the Executive Committee. External audit of the Data Security & Protection Toolkit will be undertaken by Mersey Internal Audit Agency.

6. DEVELOPMENT & CONSULTATION PROCESS

6.1 This policy has been developed by the Information Governance Manager. The policy has also been reviewed by the Caldicott Guardian, Senior Information Risk Owner and Joint SIRO and Information Governance Committee.

7. DUTIES & RESPONSIBILITIES

7.1 Chief Executive

The Chief Executive as the accountable officer is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to comply with Information Governance.

7.2 Caldicott Guardian

The Trust's Caldicott Guardian has a particular responsibility in ensuring that a robust framework to comply with all legislation is in place across the Trust. It is the responsibility of the Caldicott Guardian to ensure that ever member of staff within the Trust complies with all requirements of Information Governance, which is driven by various legislation and guidelines issued by the Department of Health and other sources.

7.3 Senior Information Risk Owner – Executive Director Finance

The Senior Information Risk Owner is responsible for ensuring that the Trust manages its information assets securely and has taken appropriate action to mitigate against any data loss/data breach incidents and that all data loss/data breach incidents are monitored and reviewed. The SIRO is the Accountable Director for ensuring that the policy is implemented.

7.4 Information Governance Manager/Data Protection Officer

The Information Governance Manager is responsible for ensuring that the Trust is working within the legal framework of the Data Protection Act 2018, EU Directive: General Data Protection Regulation, Freedom of Information Act, NHS Code of Practice for Records Management, NHS Code of Practice for Confidentiality, Data Security & Protection Toolkit Standards, NHS Digital. The Information Governance Manager is the designated Trust representative that liaises with the Information Commissioner's Office and reports data loss/data breach incidents to the Information Commissioner's Office..

7.5 Joint SIRO & Information Governance Committee

The Joint SIRO & Information Governance Committee ensures the Trust operates within the Information Governance framework and reports to the Executive Committee and provides regular Chair's Reports to the Executive Committee.

7.6 Senior Managers

It is the responsibility for all Senior Managers to ensure that staff work within the boundaries of the Trust policies and procedures and are aware of their responsibilities.

7.7 All staff

All employees of the Trust, or staff working in a voluntary capacity, independent contractors must adhere to the current legislative framework and Trust policies.

8. REFERENCE DOCUMENTS

Freedom of Information Act 2000
Data Protection Act 2018
European Directive: General Data Protection Regulation –
ICO Code of practice on the discharge of public authorities' functions underPart 1 of the Freedom of Information Act 2000 – dealing with requests for information.
ICO Code of practice on the management of records Issued under section 46 of the Freedom of Information Act 2000
The Information Governance Review – Dame F. Caldicott April 2012
The Protection of Freedoms Bill (2012)
NHS Code of Confidentiality
NHS Code of Records Management
Data Security & Protection Toolkit

Mersey Care NHS Foundation Trust Policies:-
IT10 Confidentiality and Data Sharing Policy
IT14 Data Protection Act Policy
IT04 Corporate Records Policy
IT06 Corporate Clinical Records Policy
IT13 Freedom of Information Policy
IT02 IM&T Security Policy

9. BIBLIOGRAPHY

No Bibliography

10. GLOSSARY

No Glossary

11. APPENDIX

Appendix A – Data Privacy Impact Assessment Template

Appendix A

Data Protection Impact Assessment (DPIA)

NHS Mersey Care NHS Foundation Trust
Community and Mental Health Services

This assessment should be completed as part of the business case for all new information systems and processes which involve the use of personal sensitive data or will significantly change the way in which personal data is handled.

Once the assessment has been completed, please forward to the Information Governance Team for approval – Linda.Yell@Merseycare.nhs.uk

GENERAL OVERVIEW		
1.	**Name of the new system or process:**	
2.	**Responsible Lead (name & email address):**	
3.	**What are the main aims?**	
4.	**List the main activities of the project:**	
5.	**What are the intended outcomes?**	
INFORMATION ASSET REGISTER		
6.	**Who is the Information Asset Owner - IAO(Name & email address) - MCFT staff only**	
7.	**Who is the Information Asset Administrator - IAA (name & email address) – MCFT staff only**	
DATA		
8.	**Who are the Data Subjects? (e.g.**	

	the people whose data will be held in this new system – this may be patients and/or staff)		
9.	**What Data Classes will be held on this system (ie the actual data fields)?**		
10.	**Will this system/process include data which was not previously collected?**		
11.	**Have you assessed the likelihood of data causing any unwarranted distress or damage to individuals concerned?**		
12.	**Is there a legal basis for holding and processing this data?**		
13.	**Does the system/process include new or amended identity authentication requirements that may be intrusive?**		
14.	**What checks have been made regarding the adequacy, relevance and necessity of data used?**		.
15.	**Can the system/process use pseudonyms or work on anonymous data?**		
16.	**Can the data subjects opt-out of their data being added to the**		

	system/used by the process, and if so is this publicised?		
17.	**Who are the partners for the data sharing?**		
DATA SECURITY			
18.	**Who will use the system/process and have access to the data?**		
19.	**Have or will areas involved completed the NHS Data Security Awareness module**		
20.	**Will the data be shared with any other organisations?**		
21.	**Where will data be held?**		
22.	**What format will data be stored in?**		
23.	**Does the system / process change the way data is stored?**		
24.	**How will staff access and amend data?**		
25.	**How will data be shared?**	☐ Fax ☐ Email ☐ Via NHS Mail ☐ Website ☐ Via Courier	☐ By hand ☐ Via post – internal ☐ Via post - external ☐ Via telephone ☐ Other – please state
26.	**Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)?**	☐ Yes ☐ No *If yes, please outline the data types, country, transfer methods and any measures in place to ensure adequate levels of security when transferred to this country.*	
27.	**What security measures have been taken to protect the data?**		

28.	**Is there a useable audit trail in place for the asset?** *For example, to identify who has accessed a record*	
29.	**How often will the system/process be audited?**	
30.	**Who supplies the system/process?**	
31.	**Is the supplier of the system/recipient of the data registered with the ICO? (please give registration number)**	
32.	**Has the organisation completed the NHS Digital DS&P Toolkit to a satisfactory level?**	
33.	**Does the contract include necessary IG clauses?**	
34.	**What business continuity plans are in place in the case of data loss / damage as a result of human error / computer virus / network failure / theft / fire / flood / other disaster?**	
DATA QUALITY		
35.	**Who provides the information for the asset?**	
36.	**Who inputs the data into the system?**	
37.	**How will the information be kept up to date and checked for accuracy and completeness?**	
38.	**Can an individual (or a court) request amendments or deletion of data from the system?**	.

ONGOING USE OF DATA		
39.	**Will the data be used to send direct marketing messages?**	
40.	**If yes, are consent and opt-in procedures in place?**	
41.	**Does the system/process change the medium for disclosure of publicly available information?**	.
42.	**Will the system/process make data more readily accessible than before?**	
43.	**What is the data retention period for this data?** *(please refer to the Records Management: Code of Practice for Health & Social Care 2016)*	
44.	**How will the data be destroyed when it is no longer required?**	
45.	**Does your disaster recovery solution use a 3rd party supplier?**	
46.	**Does your Disaster Recovery provider have any accreditations eg. ISO27001**	
47.	**Has your Disaster Recovery Plan been tested and was all data**	

	retained and secure?	
PIA SIGN OFF		
48.	*Your PIA should be sent to* the Information Governance Team for approval Linda.Yell@Merseycare.nhs.uk	
	Approval by SIRO / CCIO:	
	Date of PIA Approval:	
	Name of IG Approver:	
	Title of IG Approver:	
49.	**Recommendations & required further actions following PIA approval.**	

Stage 1

Rights Analysis

Title:	**Information Governance and Information Risk**
Area covered: Trust wide	

What are the intended outcomes of this work? *Include outline of objectives and function aims* To give guidance for all staff outlining their responsibilities for adhering to Information Governance and Information Risk across the organization.
Who will be affected? *e.g. staff, patients, service users etc* Staff

Evidence

What evidence have you considered?
Disability (including learning disability)
Sex
Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.*
Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*
Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.*
Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.*
Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.*
Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.*
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.*
Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to*

access.
Cross Cutting *implications to more than 1 protected characteristic*

Human Rights	**Is there an impact?** **How this right could be protected?**
Right to life (Article 2)	*Not engaged*
Right of freedom from inhuman and degrading treatment (Article 3)	*Not engaged*
Right to liberty (Article 5)	Not engaged
Right to a fair trial (Article 6)	Not engaged
Right to private and family life (Article 8)	*Not engaged*
Right of freedom of religion or belief (Article 9)	Not engaged
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	Not engaged
Right freedom from discrimination (Article 14)	Not engaged

Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.*

Summary of Analysis *This highlights specific areas which indicate whether the whole of the document supports the trust to meet general duties of the Equality Act 2010*

Eliminate discrimination, harassment and victimisation

Advance equality of opportunity

Promote good relations between groups

What is the overall impact?

Addressing the impact on equalities

There needs to be greater consideration re health inequalities and the impact of each individual development /change in relation to the protected characteristics and vulnerable groups

Action planning for improvement

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives.*

For the record

Name of persons who carried out this assessment:
Gina Kelly **Reviewed by Gina Kelly – no changes required**
Jacquie Ruddock
Kate Greenwood

Date assessment completed: 19/10/2011 **29th October 2015**

Name of responsible Director: Neil Smith

Date assessment was signed:
19/10/2011