NHS
Mersey Care
NHS Foundation Trust
Community and Mental Health Services

CONFIDENTIALITY & DATA SHARING Policy

Policy Number:	**IT10**
Scope of this Document:	**All Staff**
Recommending Committee:	**Joint SIRO &Information Governance Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**August 2018**
Next Review Date (by):	**August 2021**
Version Number:	**July 2018 – Version 6**
Lead Executive Director:	**Executive Director of Finance**
Lead Author(s):	**Information Governance Manager**

TRUST-WIDE SERVICE BASED POLICY

2018 – Version 6

Striving for perfect care and a just culture

TRUST-WIDE SERVICE BASED POLICY DOCUMENT

CONFIDENTIALITY & DATA SHARING

Further information about this document:

Document name	**IT10 – Confidentiality & Data Sharing**
Document summary	**This policy defines the framework to ensure the Trust meets its obligations in relation to the NHS Code of Confidentiality, General Data Protection Regulation 2018, Information Commissioner Officer's Code of Practice for Data Sharing**
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** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IT02 – IM&T Security Policy** **IT04 – Corporate Records Policy** **IT06 – Health Records Policy** **IT12 – Information Governance Policy** **IT13 – Freedom of Information Policy** **IT14 – Data Protection Act 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	Corporate Document Review Group	March 2012
Version 2	Corporate Document Review Group	September 2014
Version 3	Corporate Document Review Group	December 2015
Version 4	Corporate Document Review Group	February 2016
Version 5	Policy Review Group	August 2017
Version 6	Policy Review Group Minor update	July 2018 February 2020

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 / 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, sex, race, religion and belief (or lack thereof), sexual orientation, gender reassignment, pregnancy and maternity and marital and civil partnership status. The Equality Act also requires regard to socio-economic factors.

The trust is committed to promoting and advancing equality and removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those that do not 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

This policy defines the framework to ensure the Trust meets its obligations in relation to the NHS Code of Confidentiality, new Data Protection Act 2018, EU Directive: General Data Protection Regulation, Information Commissioner Officer's Code of Practice for Data Sharing.

Implementation of and adherence to this policy will ensure:

- Information is held, used, obtained and shared in accordance with the new Data Protection Act 2018, EU Directive: General Data Protection Regulation and Freedom of Information Act 2000.
- Information is safeguarded against the risk of data breach, loss, damage, destruction..
- Staff are aware of their responsibilities in respect of the NHS Code of Practice for Confidentiality, Information Governance and Data Sharing.
- This policy is applicable to all staff working for, or with, Mersey Care NHS Foundation Trust

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

- IT01 IM&T Security Policy
- IT12 Information Governance Policy
- IT14 Data Protection Act Policy
- IT13 Freedom of Information Policy
- IT06 Corporate Health Records Policy
- IT04 Corporate Records Policy

2 INTRODUCTION

2.1 RATIONALE

2.1.1 All employees working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their employment. This is not just a requirement of their contractual responsibilities but also a requirement within the new Data Protection Act 2018, European Directive: General Data Protection Regulation and, in addition, for health and other professions through their own professions Code/s of Conduct. This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. service user's and staff records. It should be noted that employees may also come into contact with non-person identifiable information which should equally be treated with the same degree of care as personal identifiable information.
.

2.2 SCOPE

2.2.1 Service users disclose sensitive personally identifiable information about themselves relating to their health and other personal matters whilst using Trust services. Personally identifiable information is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. This information includes:

- Name, address, full post code, date of birth,
- NHS number and local hospital numbers,
- Photographs, videos, audio-tapes or other images of service users
- Anything else that may be used to identify a service user directly or indirectly.

2.2.2 Service Users have a right to expect that health and any other personal information given by them, or learned by Trust staff, during the course of treatment will be regarded as confidential and kept in accordance with the law. This sensitive information is given in confidence for the provision of healthcare. Service users have the legitimate expectation that Trust staff will respect their privacy and act appropriately. This means health and social care personal information will only be used for the purpose intended and not for any other purpose without authorisation and will not be disclosed elsewhere unless, wherever possible, the service user has given their explicit and valid consent. The only exceptions to this would be in cases where there is a legal obligation to disclose or where there is evidence that disclosing the information is necessary for exceptional reasons. Without assurances of confidentiality service users may be reluctant to provide staff with the information they need to provide effective care.

2.2.3 All staff working in the Trust have a duty to respect the confidentiality of service user information, and not to divulge it to anyone who is not immediately concerned with the care of the service user. Any breach of confidentiality is regarded as extremely serious and may result in disciplinary action or dismissal. Clinical staff that are alleged to have breached confidentiality will also be reported to the appropriate disciplinary committee of their professional body. The duty of confidence may be legally enforceable by the service user, either through an injunction or a civil action for damages.

2.2.4 This Code has been written to meet the requirements of:

- The new Data Protection Act 2018
- European Directive: General Data Protection Regulation
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- NHS Code of Confidentiality
- ICO Code of Practice for Data Sharing
- Caldicott reviews and principles

2.2.5 The code aims to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of those requirements and must be read in conjunction with the Trust Data Protection Act Policy, Information Governance Policy, Corporate Health Records Policy, Freedom of Information Act Policy.

2.2.6 This policy applies to:-

- All staff –permanent, temporary and those with honorary contracts.
- All third party contractors working in or for the trust and
- All partner organisations sharing services.

2.2.7 It operates at all times from referral and recruitment to beyond discharge and retirement through the complete lifecycle of care plan assessment and working practice.

2.3 PRINCIPLES

2.3.1 In accordance with the NHS Code of Confidentiality, new Data Protection Act 2018, EU Directive: General Data Protection Regulation, and Caldicott Principles, Mersey Care NHS Foundation Trust is committed to the delivery of a first class confidential service. This means ensuring that all service user information is processed fairly, lawfully and as transparently as possible so that service users and staff:-

- Understand the reasons for processing personal information
- Give their consent for the disclosure and use of their personal information
- Gain trust and confidence in the way the Trust handles information and;
- Understand their rights to access information held about them.

2.3.2 The Caldicott Principles underpin the legal and ethical obligations of confidentiality.

2.3.2.1 <u>Justify the purpose(s)</u>

Every proposed use or transfer of person-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian.

2.3.2.2 <u>Don't use person-identifiable information unless it is absolutely necessary.</u>

Person-identifiable information items should not be used unless there is no alternative.

2.3.2.3 Use the minimum necessary person-identifiable information

Where use of person-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

2.3.2.4 Access to person-identifiable information

Only those individuals who need access to person-identifiable information should have access to it, and they should only have access to the information items they need to see.

2.3.2.5 Everyone should be aware of their responsibilities

Action should be taken to ensure that those handling service user-identifiable information – both clinical and non-clinical staff are aware of their responsibilities and obligations to respect confidentiality.

2.3.2.6 Understand and comply with the law

Every use of person-identifiable information must be lawful. The Information Governance Manager is responsible for ensuring that the organisation complies with legal requirements.

2.3.2.7The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

3 POLICY

3.1 Information provided in confidence should not be used or disclosed in a form that might identify the service user or member of staff without their consent. There are some important exceptions to this rule detailed in section 3.

3.2 The NHS Confidentiality Code of Practice describes fully the duty of confidence arising when one person discloses information to another for e.g. in circumstances where it is reasonable to expect that the information will be held in confidence. It –

a) is a legal obligation that is derived from case law;
b) is a requirement established within professional codes of conduct;
c) must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures;
d) must be included in third party contracts; and
e) must be included in information sharing agreements.

Overall corporate requirement for confidentiality and data sharing

3.3 Staff

This section describes individual responsibility of people working for the Trust. This includes permanent, temporary, locum, and workers with limited honorary contracts, described throughout this policy as "all staff".

3.4 Contracts of Employment, Staff Handbook & Whistle Blowing

The extract below is part of an individual's contract of employment reflecting the Trust's Policy regarding Confidentiality.

3.4.1 "Duty of Confidence"

As a Mersey Care NHS Foundation Trust employee you have a legal duty of confidence to service users and breaching that confidence can be a serious disciplinary offence.

3.4.2 You must not whilst you are employed or after your employment ends, disclose to any unauthorised person information concerning the Trusts' business or the service users in it's care; nor must you make a copy, abstract, summary or précis of the whole or part of a document relating to the Trust. You are required to obtain the prior approval of the Trust to deliver any lecture or publish any article relating to your official duties. You have a right and a duty to raise concerns about health service issues with your Manager.
A Trust Staff Code of Conduct in respect of Confidentiality has been developed and is attached at the back of this policy. (See Appendix A)

3.4.3 Freedom to Speak Up including Whistleblowing

The Trust has a policy on concerns at work about service user care or matters of business probity/conduct. As a member of staff you may be worried about raising such issues or may want to keep the concerns to yourself, perhaps feeling it's none of your business or that it's only a suspicion. Issues raised under this policy will, wherever possible, be dealt with as per policy guidance and in a way that produces speedy and effective outcomes, which minimise the risk of any breach of confidentiality. Please refer to the Trust policy HR06 – Freedom to Speak Up including Whistleblowing.

3.4.4 Social Media

Staff must not post any information regarding service users, Staff or Trust business on social media sites or information as this may breach Data Protection legislation or cause reputational damage to the Trust.

3.5 Induction

All new staff will be required to complete the mandatory Data Security Awareness on-line training module. Individual sessions will be organised for staff who have specific requirements. Staff are issued with their Mersey Care NHS Foundation Trust identity badges and advised to wear them at all times.

3.6 **Corporate Essential Mandatory training/Specialist Training**

To maintain awareness of confidentiality and data sharing all staff will be required to complete the on-line annual Data Security Awareness module annually with additional procedures and guidance available via the trust Information Governance intranet or trust website.

3.7 **Access to Information Systems**

No-one should seek or be granted unauthorised access to any staff or service user information system. Existing procedures allow role based access to existing databases. When staff leave, for whatever reason access to sensitive personal information should cease, in some cases immediately.

3.8 **Staff access to their own records**

Staff are entitled under the Data Protection Act and General Data Protection Regulation Subject Access Rights. However, staff **must** follow the Trust's formal Data Protection Act Policy and Procedure. Staff **must not** access their "own" records without following the Trust Data Protection Act policy as this would be considered a breach of their position and lead to disciplinary action. In some circumstances, responding to a request from a member or ex-member of staff may involve providing information relating to another individual who can be identified from that information (third party information). This can give rise to conflict between the data subject's right of access and the third party's right to respect of his/her private life. Third party information must be removed or anonymised if the third party has not provided their consent.

3.9 **Non Permanent Staff**

Where a non-NHS agency or individual is contracted to carry out or support NHS functions, the contract must specify appropriate confidentiality and security requirements. The contractor must protect personal data in accordance with the provisions and principles of the Data Protection Act and General Data Protection Regulation, in particular the contractor must ensure compliance with the Trust's security arrangements and ensure the reliability of its staff who have access to any personal data held by the Trust. In addition, if the contractor is required to access or process personal data held by the Trust, the contractor shall keep all such personal data secure at all times and shall only process such data in accordance with instructions received from the Trust.

3.9.1 As part of the security arrangements, all non-permanent staff must carry a letter of authorisation identifying themselves and their purpose and timeframe.

3.10 **Security of all Trust Information**

There are three elements:

3.10.1 **Confidentiality** – only people who are authorised to process data can access it.

3.10.2 **Integrity** – personal data should be accurate and suitable for the processing purpose and

3.10.3 **Availability** – authorised data users should be able to access necessary data.

3.11 **User Responsibility**

Following Corporate Induction, line managed local induction reinforces essential messages:

- Understanding of this policy
- Where to go for further information
- How to access expertise within the Trust
- If in doubt seek help
- Focus on Caldicott principles
- Responsibilities will lead to judgements on a case-by-case basis
- Record all unusual disclosures
- Ensure that staff know if they follow the policy they will be Supported

3.12 **Information Security Policy**

This policy must be understood as it details the legislative framework for securing confidential information and that only by appropriate reporting of incidents involving loss or breach of confidentiality can the Trust maintain its high standards for ensuring safety and security of its information.

3.13 **Monitoring & Reporting Incidents**

The methodology to use is outlined in the Adverse Incident Policy. Reports in respect of data loss or breaches are monitored by the Joint Senior Information Risk Owner Group/Information Governance Committee with this information being cascaded to Divisions for action. The Senior Information Risk Owner provides regular Executive Summary reports to the Executive Committee.

3.13.1 In the event of any concerns raised regarding service users current health status the Division/clinical team supporting the service user must be contacted so that the appropriate care and support can be implemented.

3.14 **Specialist Advice in respect of Confidentiality & Data Sharing**

This can be accessed by contacting the Information Governance team at Mersey Care NHS Foundation Trust on 0151 471 2686/2351 or via email to Linda.Yell@Merseycare.nhs.uk

3.15 **Service Users**

3.15.1 **Information on entry**

It is extremely important that service users are made aware of information disclosures that must take place in order to provide them with high quality care. In particular, service governance and clinical audits, which are wholly proper components of healthcare provision,

might not be obvious to service users and should be drawn to their attention. Similarly, whilst service users may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not be the case and the efforts made to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies.

There are a range of uses of confidential service user information that do not contribute to or support the healthcare that a service user receives. Very often, these other uses are extremely important and provide benefits to society – e.g. Medical research, protecting the health of the public, health service management and financial audit. However, we cannot assume that those service users are content for their information to be used in these ways.

3.15.2 Accuracy checking

It is of vital importance that staff regularly check demographic data with the service user and update any changes. In the event of any errors being identified in respect of record keeping or data quality then these must be rectified as soon as possible which may involve notification to the Data Quality team.

3.15.3 Copying Correspondence

Health and Social Care professionals have been providing copies of documentation to service users and carers for many years. This documentation normally includes assessment of need, the care pathway, contingency plans and risk assessments.

Mersey Care NHS Foundation Trust clinicians also prepare detailed reports for the purpose of mental health review tribunals, which are routinely made available to the service user.

The Trust has a policy in place regarding Copying letters to service users. Whilst the Trust enthusiastically supports sharing copies of letters to service users, the rules of Data Protection legislation apply and there are some exceptions that exist where the service user or others could be seriously harmed.

3.15.4 Service User Access to their information

The new Data Protection Act 2018 and General Data Protection Regulation provide individuals (Data Subjects) with the right to access their personal data. A health record is defined as being any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of the individual.

The Access to Health Records Act 1990 has now been repealed except for sections dealing with requests for access to records relating to deceased individuals. NHS records are public records and relate to **all types of records** including:

- patient health records (electronic or paper based concerning all specialties);
- Accident and Emergency, birth and all other registers;
- Theatre registers and minor operations (and other related) registers;
- Administrative records (including, for example, personnel, financial, estates);
- X-ray and imaging reports, output and images;
- Photographs, slides and other images;
- Microform (microfiche/microfilm);
- Audio and video tapes, cassettes, CD-ROM;
- CCTV footage
- Emails;
- Computerised records;
- Scanned records;
- Text messages (both outgoing messages from the NHS and incoming responses from the patient)

3.16 Is this a subject access request?

Any verbal, written or via social media request specifying the individual requires access or copies of their personal information held or processed by the Trust should be processed as a subject access request. The request must contain sufficient information to enable the Trust to conduct the search required e.g. Name, Address and Date of Birth.

3.17 Subject Access Process

Requests can be in writing, verbal or by social media with the trust providing assistance to individuals who may have difficulty completing the application form. Applications can be from various sources including: solicitor's requests which should be accompanied by a signed disclaimer, patient's Medical Insurance Companies and the Police. The Applicant (data subject) must provide enough information for the Trust to be able to process the request. For further information please see the Trust Data Protection Act policy.

3.18 Disclosure of Personal Information

The following guidance is derived from the Department of Health NHS Code of Practice for Confidentiality. This document is the current guidance to required practice for everyone subject to this policy concerning confidentiality and service users' consent to the use of their health and social care records. The Code is also relevant to anyone working in and around health and social care. This includes private and voluntary sector staff and as such stands as common expectations of sharing.

3.19 Sharing for Health and Social Care purposes

This most commonly used model describes most of our day to day actions, describing generally consenting business of sharing within our caring community and describes disclosures to other NHS staff involved in the provision of healthcare, to social workers or other staff

of non-NHS agencies involved in the provision of healthcare, to parents and guardians and to carers.

This model also covers clinical audit. The evaluation of clinical performance against standards or through comparative analysis, with the aim of informing the management of services is an essential component of modern healthcare provision.

3.20 Disclosing for other Medical purposes

This model generally requires consent before disclosing to researchers, to NHS Managers and/or the Department of Health, e.g. commissioning, financial audit, resource allocation etc., to Occupational Health Practitioners, to bodies with statutory investigative powers – General Medical Council, Healthcare Commission, Audit Commission, NHS Complaints Committees.

In exceptional circumstances the Patient Information Advisory Group (PIAG) under Section 60 of the Health and Social Care Act 2001 uses a power to ensure that service user identifiable information needed to support essential NHS activity can be used without the consent of service users.

3.21 Research Governance

Unlike Clinical Audit (3.4.1), there are stringent arrangements when engaging service users in research. The Trust Research Governance Committee ensure appropriate measures are in place including Information Governance requirements to which the proposing research must agree. This includes informed consent, data security, and reuse of data.

3.22 Unrelated to health and social care

This is the model where there must be a justification for disclosure. Two specific groups are described below: the Media 3.4.5 and the Police 3.5.1

The model covers information to Hospital Chaplains, for non-statutory investigations, to Government Departments, to the Police, required by a Court including a Coroner's Court, Tribunals and Inquiries, to the media and to NHS solicitors.

3.23 Media specific

All staff should refer any press or other media issue or question directly to the Trusts Communication Department. All media outlets should know through operational practice that they address their questions this way. Any member of staff receiving a communication from the media can reinforce this route. Therefore, all staff should work secure in the knowledge that the Trust has a department dedicated to this task.

3.24 Exceptions

If the public good serviced by disclosure is significant, there may be grounds for disclosure. The key principle to apply here is that of proportionality.

The new Data Protection Ac 2018 and General Data Protection Regulation allows for disclosure without the consent of the subject in certain conditions, including for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, and where failure to disclose would be likely to prejudice those objectives in a particular case.

Disclosure should be justifiable in each case, according to the particular facts of the case, and legal advice should be sought in cases of doubt. Disclosure should be appropriate for the purpose and only to the extent necessary to achieve that purpose.

3.25 **Public Interest**

Any staff member on a case-by-case basis, in any circumstance, who takes the decision to use an exemption and disclose information, must record the fact so that there is clear evidence of the reasoning used and the circumstances prevailing. It is important not to equate "the public interest" with what may be "of interest" to the public.

3.26 **Serious Crime and National Security**

The definition of **serious** crime is not entirely clear. Murder, manslaughter, rape, treason, kidnapping, child abuse or other cases where individuals have suffered serious harm may all warrant breaching confidentiality. Serious harm to the security of the state or to public order and crimes that involve substantial financial gain or loss will also generally fall within this category. In contrast, theft, fraud or damage to property where loss or damage is less substantial would generally not warrant a breach of confidence.

3.27 **Police Specific**

The Police with partner agencies detailed in their Protocol (5.5 below) share our duty within the NHS to protect individual's information, but recognising that "the ability to exchange information is critically important". The protocol recognises that legitimate requests for information are managed by designated roles. In the Police Service these are the inter-agency police liaison officers. During each day policing within the Mersey area has an inter-agency liaison office whose job relates to sharing information. During the evening, night and weekends there is always a force incident manager on duty.

3.27.1 Mersey Care mirrors these responsibilities in the table below. All requests for information from the police will be routed to the Service Manager or Silver On call. Similarly if the Trust seeks information it will be through the Service Management or on call process. However, for high security exchanges, please refer to the "Referral to the Police"

	To the Police via	**From the Police via**
9.00am to 5.00pm	Service Manager or Complaints Manager for Secure Division	Inter-agency Police Liaison Officer.

5.00pm to 9.00am & weekends	Silver On call	Force Incident Manager

3.28 **Risk of Harm**

Disclosures to prevent serious harm or abuse also warrant breach of confidence. The risk of child abuse or neglect, assault, a traffic accident or the spread of an infectious disease are perhaps the most common that staff may face. However, consideration of harm should also inform decisions about disclosure in relation to crime. Serious fraud or theft involving NHS resources would be likely to harm individuals waiting for treatment. A comparatively minor prescription fraud may actually be linked to serious harm if prescriptions for controlled drugs are being forged. It is also important to consider the impact of harm or neglect from the point of view of the victim(s) and to take account of psychological as well as physical damage. For example, the psychological impact of child abuse or neglect may harm siblings who know of it in addition to the child concerned.

3.29 **Child Protection**

Research and experience have shown repeatedly that keeping children safe from harm requires professionals and others to share information; about a child's health and development and exposure to possible harm; about a parent who may need help to, or may not be able to, care for a child adequately and safely; and about those who may pose a risk of harm to a child. Often, it is only when information from a number of sources has been shared and is then put together that it becomes clear that a child is at risk of suffering significant harm.

- You have a duty to act if you think a child is at risk
- You do not need evidence of abuse, just a reasonable belief that a child is at risk
- You can disclose confidential information about a child to the police or social services without parental authority if it is needed to safeguard a child, but it should be the minimum information necessary and given on a need to know basis.
- Be aware of your local child protection procedures and of relevant guidance such as that from the Royal College of Paediatrics and Child Health.

3.29.1 Normally, personal information should only be disclosed to third parties (including other agencies) with the consent of the subject of that information, including the child where they are of sufficient age and understanding. Wherever possible, consent should be obtained before sharing personal information with third parties. In some circumstances, obtaining consent may neither be possible nor desirable but the safety and welfare of a child may dictate that the information should be shared without consent.

3.30 Safeguarding

Recognition of suspected or actual abuse of service users is the responsibility of all staff within Mersey Care NHS Foundation Trust.

When considering whether to disclose information to a third party, it will be necessary to identify the circumstances in which the practice of respecting confidentiality should be overridden in order to protect the service user. Examples of this may either be where a vulnerable adult is being intimidated or where there is concern about the risk to another vulnerable adult.

The Protection of Vulnerable Adults Scheme (POVA) came into force in July 2004. At the heart of the scheme is the POVA list. Care workers are referred to the list if they have harmed, or put at risk of harm, a vulnerable adult in their care. This is the case for Mersey Care workforce. In short, POVA is a workforce ban that will be one means of ensuring that known abusers who have abused or mistreated vulnerable adults in their care do not remain in the workforce or find their way back into such positions again.

3.31 Legally Required

Some statutes place a strict requirement on clinicians or other staff to disclose information. Care should be taken however to only disclose the information required complying with and fulfilling the purpose of the law. If staff have reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the service user or another person they should seek further advice from the Trust Information Governance Manager who may seek further legal advice.

3.31.1 The Courts, including Coroner's Courts, and some tribunals and persons appointed to hold inquiries have legal powers to require that information that may be relevant to matters within their jurisdiction be disclosed. This does not require the consent of the service user whose records are to be disclosed but they should be informed preferably prior to disclosure. Disclosures must be strictly in accordance with the terms of a court order and to the bodies specified in the order. Where staff are concerned that a court order requires disclosure of sensitive information that is not germane to the case in question, they may raise ethical concerns with the judge or presiding officer. If however the order is not amended it must be complied with.

3.31.2 Legal Restrictions on Disclosure of Sexually Transmitted Diseases

Existing regulations require Mersey Care NHS Foundation Trust to take all necessary steps to secure that any information capable of identifying an individual obtained by any of their members or employees with respect to person's examined or treated for any sexually transmitted disease (including HIV and AIDS) shall not be disclosed except:

1. where there is explicit consent to do so
2. for the purpose of communication that information to a medical practitioner or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof, and
3. for the purpose of such treatment or prevention.

It is clear that many service users would regard information about Sexually Transmitted Diseases as particularly sensitive and private. It should never be assumed that service users are content for this information to be shared unless it has a direct and significant bearing on their healthcare and where the regulations apply it must not be disclosed other than as described above.

3.32 **Legally Permitted**

Legislation may also create what are termed 'statutory gateways' that allows information to be disclosed by the Trust e.g. section 115 of the Crime & Disorder Act 1998. As these gateways are opened appropriate guidance or instruction will be issued.

3.33 **Information Sharing & Using**

This policy will enable the Trust, its staff members and service users to understand that data sharing can take place in a way that helps deliver a better service, while still respecting people's legitimate expectations about the privacy and confidentiality of their personal information.

3.33.1 Where personal accountability to a code of conduct does not apply then staff should be aware that complete confidentiality couldn't be offered to an individual. Information given to an individual member of staff belongs to the Trust and not to the staff member alone and should be shared on a 'need to know' basis with other Trust colleagues, for example with a line manager.

3.33.2 It will always be difficult to make decision about whether to share (or not to share) information about risk, particularly where the issue is about disclosing to individuals or voluntary bodies. It will always be crucial to gather the best information possible about the risk posed, assess the risk and consult thoroughly before reaching a decision.

3.34 **Lawful Sharing**

Information sharing takes place in most of our work. Exemptions are described above. If the following conditions apply sharing is lawful.

1. If the data collection and sharing is to take place with the consent of the service user involved, Article 8 of the Human Rights Act will not be engaged. This 'Article' guarantees respect for four things: a person's private life, family life, home and correspondence. This is the essence outlined in this policy. When Article 8 of the European Court of Human Rights is engaged, then sharing is in accordance with the law, principally the Mental Health Act and is in pursuit of a legitimate aim. So for our purpose we can share information.

2. Again if the data collection and sharing is to take place with the consent of the service users involved, the information will not be confidential and we can proceed.

3. The Trust's notification to process information for health and social care purpose's is registered with the Information Commissioner. This allows the sharing of information as part of that process. The Information Commissioner also makes the specific point that the statutory requirements of our Mental Health legislation may take precedence over common law.

4. If the Trust has signed up to a formal Data Sharing Agreement with another organisation for the provision and exchange of healthcare, the service users will be made aware of the shared care provision and information exchange.

5. All exemptions are described in the previous section of this policy (3.5)

6 Any queries regarding confidentiality and information sharing should be through the Information Governance Manager for best practice.

3.35 **Competence to Consent**

Seeking consent of service users may be difficult due to illness, disabilities or circumstances that may prevent them from becoming informed about the likely uses of their information. The Mental Health Capacity Act (2005) intends to protect people who lose the capacity to make their own decisions. The Act allows the person, while they are still able, to appoint someone (for example a trusted relative or friend) to make decisions on their behalf, in their best interests, for their health and personal welfare, not just financial matters, once they lose the ability to do so. Mental Capacity Act (2005) introduces a Code of Practice for healthcare workers who support people who have lost the capacity to make their own decisions. Staff should refer to this guidance when making decisions about access to information of service users. If the service users nominated a legal representative (attorney or deputy) to be involved in decisions about their care should they become incapacitated, only relevant information can be shared with that person, provided they prove their official authority (proof of ID and appointment). Disclosures should not include information about third parties. Where the service user is incapacitated and unable to consent, information should only be disclosed in the service user's best interests. It is essential that only Information that is needed to support their care is disclosed. If a service user has made their preferences about information disclosures known in advance, this should be respected. In some circumstances, service users may have a difficulty communicating their decision to consent or object. It is important to check for a clear and unambiguous signal of what is desired by the service user, and to confirm that the interpretation of that signal is

correct by repeating back the apparent choice. See Trust Consent Policy for further information.

3.36 Information Flows

It is important to develop a thorough understanding of how information is being used within the Trust. This will ensure compliance with the Data Protection Act, General Data Protection Regulation about adequacy and relevance and the Caldicott principle of 'justification'. The Data Security & Protection Toolkit also requires Trust's to conduct annual information data flow mapping to ensure that the correct safeguards are in place to protect the flow of personal identifiable information.

3.36.1 Anyone who routinely dispatches personal information either about individuals or as lists must review their distribution; both recipients and method. Anyone with a concern about the flow of information should make their concerns known to the Trust Information Governance Manager.

3.37 Meetings Protocol

From the Care Programme Approach to Research Governance and Adverse Incidents, many meeting documents contain personal and perhaps sensitive information. All committees and teams must consider their documentation and be aware of confidential references. They can work to reduce the amount of confidential material and collect papers, which have served their purpose at the end of the meeting to reuse or recycle confidentially.

3.38 Information Sharing Agreements

The Information Commission published a Code of Practice in May 2011 in respect of Data Sharing. There are some organisations that the Trust regularly shares data with e.g. Safeguarding Teams – Social Services, Addaction Service and Addictions, other NHS trusts. Specific Data Sharing Agreements are in place that state what data will be shared, its specific purpose and the responsibilities for staff training, policies, procedures and reporting process for any breaches of confidential information or data loss. All Information Sharing Agreements (also known as Data Sharing Agreements) are co-ordinated and implemented by the Information Governance Manager, with sign off by the Caldicott Guardian and in some cases the countersignature of the Chief Executive. A central log of organisations that have Data Sharing Agreements in place with the Trust is held by the Information Governance Manager.

3.39 Privacy Impact Assessments

In order to safeguard personal identifiable information at the start of planning new projects or introducing operational changes that involves the processing or use of personal identifiable information a Data Privacy Impact Assessment must be completed and submitted to the Information Governance Manager. A copy of the Privacy Impact Assessment is attached at the back of this policy (see Appendix B)

3.40 Objections from Services Users to disclosure of information

In the event that a service user has concerns in respect of their personal information being disclosed to another agency then the service user should discuss this with their health and social care professional.

3.40.1 A decision must then be made by the responsible health or social care professional in relation to the clinical detail provided to other agency and the level of risk posed to the individual service user or others if information is not disclosed.

The justification for any disclosures should be clearly documented and the reasons for going against the service users wishes clearly explained to the service user

3.41 **Complaints, Claims & Incidents**

This section focuses on activities, which routinely access, record and report sensitive information. Inappropriate use of privileges is often found to be a major contributory factor to the failure of systems that have been breached. In noting this, the information security management code of practice raises two objectives:

a) To ensure that access rights are appropriately authorised, allocated and maintained and
b) To prevent unauthorised access to information.

3.41.1 Service users and staff rightly expect high levels of control in these areas. Privileged access brings responsibility and consideration of the risks in the long term. The over use of personal and sensitive information in our reports, bring less control and a greater risk of breach, especially if the report is shared across a wide distribution.

3.41.2 Therefore, information usage must be scrutinised for justification, on a need-to-use, need-to-know and event -by-event basis; e.g. the minimum requirement only.

3.41.3 The only other rule is to be clear about identifying an individual. This will vary across the range of reports but if an individual's identity is necessary for the report then it is justified. If the information is used for a different purpose or different audience then the justification ceases and anonymity must be established.

To satisfy the code's requirements, the managers of these services have a responsibility to ensure those staff with privileges or reporting responsibilities follow this policy.

3.42 **Transfer Of Information**

How the information is to be transferred will depend upon how it is held currently, the type and volume of information to be shared and appropriate date range of information to be shared. The transfer method of all personal identifiable information must be secure.

3.42.1 However, consideration of the re-attendance rates of the service need to be taken into account and appropriate 'back data' may also need to be transferred.

3.42.2 The information that is transferred should be in accordance with the Data Protection Act 2018, EU Directive: General Data Protection Regulation and sufficient to allow continuity of patient care but not excessive.

3.42.3 The transfer of the information should be done in accordance with the Data Protection Act, EU Directive: General Data Protection Regulation and Caldicott Principles i.e. to ensure confidentiality and security of the information is maintained at all times. If an electronic transfer then the IM&T Security team can assist and advise at both the receiving and transmitting ends should be involved to ensure that this is adhered to.

3.42.4 If paper records are to be transferred then the transmitting organisation must retain the original records (as they were the data owner at the time of creation). The cost of facilitating the copying of these records should be included in costs of the contract and therefore borne by the receiving organisation on the basis that they have obtained the monies to take the service forward.

3.42.5 **National Data Opt Out**

A secure and accessible tool for people to opt-out of their confidential patient information being used for reasons other than their individual care and treatment is available. This means patients have more control over how their information is used and gives them the opportunity to make informed choices about whether they wish their confidential patient information to be used just for their individual care and treatment or also used for research and planning purposes. Further information is available at https://www.nhs.uk/your-nhs-data-matters/. When necessary, the Trust applies the Policy to its data.

You can also opt-out of the national screening programmes. For further information, please go to https://www.gov.uk/government/publications/opting-out-of-the-nhs-population-screening-programmes.

4. MONITORING & REVIEW

Monitoring and review of this Policy will take place by the Joint SIRO and Information Governance Committee on a bi-monthly basis. An Information Governance Chair's report providing an overview of Information Governance matters will be provided to the Executive Committee for review on a bi-monthly basis.

5. DEVELOPMENT & CONSULTATION PROCESS

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 members of the Joint Senior Information Risk Owner/ Information Governance Committee.

6. DUTIES & RESPONSIBILITES

6.1 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 and all current legislation.

6.2 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.

6.3 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 responsible for ensuring that the policy is implemented.

6.4 Information Governance Manager/Data Protection Officer

This person 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, Information Governance Standards. The Information Governance Manager is the trust designated individual who liaises with the Information Commissioners Office.

6.5 Joint Senior Information Risk Owner/Information Governance Committee

The Joint Senior Information Risk Owner/Information Governance Committee ensure that the Trust operates within the Information Governance framework and is accountable to the Trust Executive Committee.

6.6 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.

6.7 All staff

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

7 Training

Training is provided to staff in respect of Confidentiality during Induction and Local Induction in the work area. Guidance is also provided on all Job Descriptions and Trust Policies. Reminders in respect of confidentiality and Information Governance are on "screenshots" at system log-on. Prior to staff being provided with "live access" to the Clinical Information Systems they are made aware of their duties in respect of the NHS Code of Confidentiality and the Data Protection Act. All staff are required to complete the Mandatory Data Security Awareness e.Learning module.

8. REFERENCE DOCUMENTS

Freedom of Information Act 2000
Data Protection Act 2018
European Directive: General Data Protection Regulation
ICO – Code of practice for Information Sharing
Record Management and Management of Records Policies
IM&T Security Policy

9 BIBLIOGRAPHY

No Bibliography

10. GLOSSARY

No Glossary

11. APPENDIX

Code of Conduct in respect of Confidentiality – Appendix A
Privacy Impact Assessment – Appendix B

Appendix A

INFORMATION GOVERNANCE – STAFF CODE OF CONDUCT

Professional Code of Confidentiality

1 Introduction

1.1 All employees working in the NHS (Non-Executive Directors, temporary, permanent, contractors, students and agents) are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. The disclosure and sharing of personal identifiable information is governed by the legislation and professional codes of conduct:

- Data Protection Act 2018
- European Directive: General Data Protection Regulation 2018
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Common Law Duty of Confidentiality.
- Confidentiality: NHS Code of Practice Nov.2003
- Access to Health Records 1990
- Freedom of Information Act 2000

Further information can be found in the Department of Health's Confidentiality NHS Code of Practice.

1.2 This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient/service user and employee records. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of care e.g. business in confidence information, such as referral letters, discharge summaries, waiting list data, clinic lists as well as some corporate or administration reports which contain confidential information.

1.3 Mersey Care NHS Foundation Trust is committed to the delivery of a first class confidential service and this Code of Practice has been developed to establish good working practices that effectively deliver patient/service user confidentiality that is required by statue, common law, government guidelines and information sharing protocols.

1.4 This Code of Practice is based on "Confidentiality: NHS Code of Practice" produced by Department Health. This code of Practice has been endorsed by the GMC, BMA, MRC and the Information Commissioner.

1.5 The Code of Practice is a requirement of NHS Digital and contained within the Data Protection & Security Toolkit.

2 Purpose

2.1 The main purpose of this Code of Practice is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of Mersey Care NHS Foundation Trust security systems or controls in order to do so.

3 Roles & Responsibilities

3.1 The Caldicott Guardian

- ensures the Care Trust and its partner organisations satisfy the highest practical standards for handling patient/client information
- Acts as the "conscience" of the organisation
- Actively supports work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required

3.2 The Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is the Executive Director for Information, Performance and Improvement who is a Management Board Member and has:-

- overall ownership of the Organisation's Information Risk Policy
- to act as champion for information risk on the Board
- provides written advice to the Trust Board on the content of the Organisation's Statement of Internal Control in regard to information risk.

3.3 The Information Governance Manager/Data Protection Officer

supports the Caldicott Guardian and Senior Information Risk Owner in all matters of confidentiality, data sharing, current legislation and data loss/breach incidents on a day to day basis.

3.4 **Line Managers** are responsible for ensuring that:

- Staff comply with this Code of Practice and report all breaches and suspected breaches of confidentiality in accordance with the Trust's Adverse incident reporting policy.
- All staff understand Information Governance, their responsibilities and the duty of confidentiality as stated within their contract of employment.
- Temporary, agency, honorary contract staff including volunteers, service users & carers are made aware of this Code of Practice, in particular their own responsibilities for compliance.

All **employees** are responsible for:

- Ensuring that they are aware of the requirements of confidentiality and for ensuring that they comply with these on a day to day basis.
- Ensuring that information whilst in their possession, particularly personal and sensitive information is kept safe and secure at all times, (including photos, videos and audio recordings). This includes mobile phones, laptops, paper records, emails, etc.
- Ensuring they are not placed in the position which risks, or appears to risk, conflict between their private interests and the NHS duties. Further information can be found in on the Trust website and its policies relating to Standards of Business.
- If there is the need to take personal information home, then this information must be secured against accidental disclosure.
- Information must be securely managed by staff transporting or using personal identifiable information away from trust premises.
- To report any suspected breaches of confidentiality, loss of data immediately to their line manager and through the Datix incident reporting procedure.
- Ensuring that all work related passwords and pin numbers are kept confidential, safe and secure at all times. (See Section 6.10 for additional information).
- No employee shall knowingly misuse information or allow others to do so. Breach of confidentiality is a serious concern and failure to adhere to the Code of Practice and associated guidance may result in disciplinary action being taken in accordance with the Disciplinary Policy, and may lead to dismissal for gross misconduct.
- Any queries relating to the use and disclosure of confidential information may be referred to the Information Governance Team.

4 Definition of Personal and Confidential Information

4.1 Information may be held on paper, CD/DVD, memory stick, other portable media, or as a printout, email, video, photograph, audio recording or even heard by word of mouth. It includes information stored on portable devices such as laptops, palmtops, memory sticks, mobile phones, digital cameras, etc. It can take the form of clinical care records, audits, employee records, etc. It also includes any Trust corporate and administration confidential information. Further information on what is a record/information can be found in the Records Management Policy.

4.2 Confidential Information

- Confidential information is information that relates to service users, staff (including non-contract, volunteers, bank and agency staff, locums and student placements), their family or friends, however stored (paper, electronic, DVD, photos, videos, audio recordings, CD, print out or even heard by word of mouth).
- It includes information stored on portable devices such as laptops, palmtops, mobile phones, ipads, iPhones, smart phones and digital cameras.

- Any clinical or care records, audits, employee records, occupational health records, etc. It also includes any confidential information relating to the organisation.
- Business and Corporate records, including administration records containing information about the day-to-day business of the Trust or future developments in service planning may contain information that is classed 'confidential'.

4.3 **Personal and Sensitive Information**

4.3.1 Personal-identified information is anything that contains the means to identify an individual, e.g. name, address, postcode, date of birth, NHS number, NI number, photograph, etc. A list can be found in Appendix 2. Please note a visual image, such as a photograph or video, is sufficient to identify an individual.

4.3.2 Certain categories of information are legally defined as particularly sensitive and should be carefully protected by additional requirements e.g. regarding in-vitro fertilisation, sexually transmitted diseases, HIV and termination of pregnancy.

4.3.3 During an employee's duty of their work, they should consider all information to be sensitive, even something such as a patient's name and address. The same standards should be applied to all information you come into contact with.

4.4 **Anonymised Information**

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full postcode and any other detail or combination of details that might support identification.

4.5 **Pseudonymised Information**

This is like anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However it differs in that the original provider of the information may retain a means of identifying individuals.

5 Disclosing and Using Confidential Information

5.1 Service Users must be made aware of information disclosures that have to take place in order to provide them with high quality care, particular if information is being disclosed to non NHS bodies.

5.2 **Sharing with Consent**

5.2.1 Staff should ensure that informed consent to share personal sensitive information (for example health records) is gained at each episode of care and clearly recorded.

5.2.2 Sensitive information (for example medical information) will only be released if its disclosure is deemed critical to the case by the appropriate health/social care professional and informed consent has been given to release for that purpose. Consent should be clearly recorded.

5.3 **Sharing without Consent**

5.3.1 If an individual has refused consent to share some of all of their information, it may mean that the care being provided is limited and, in rare circumstances, it may not be possible to offer certain treatment options. This must be explained clearly to the individual so that they are fully informed of the effect that this may have on their care and treatment.

5.3.2 In some cases it may not be practical to obtain consent, for instances if the individual is unable to give consent, there may be a risk to third party or may result in harm to an individual, including a work colleague, or may prejudice the detection and/or investigation of a crime.

5.3.3 If an individual is unable to give consent, the decision should be made on the individual's behalf by the health/social care professional responsible for providing care, taking into account the views of the individual, their families and carers. The best interests of the individual should be paramount at all times.

5.3.4 If an individual is a child then the Gillick competency and Fraser guidelines should be taken into account to gain the necessary consent to share. This will depend upon the child's maturity and understanding. The child must be capable of making a reasonable assessment of the advantages and disadvantages of the proposed information sharing.

5.3.5 Legislation and guidance outlined in section 1 and appendix 2 must be taken into account when making a decision to share personal sensitive information.

5.3.6 If you are unsure as to whether you can disclose the information requested please seek advice from your professional lead, line manager or the Information Governance Team.

5.3.7 Recipients of personal information which has been shared without consent will be informed of the consent status. They will also be informed on what basis the decision to share was made and will put in place agreed security procedures.

5.3.8 The individual should be informed of any disclosure made without consent, unless there are justifiable concerns for the safety of an individual or others. If there are concerns, then the individual will not be informed of the relevant disclosure.

5.3.9 In all cases, when personal and/or sensitive information is shared, either, with or without consent, a record of the sharing event should be kept on file as soon as possible after the event clearly stating what information was disclosed, who it was disclosed to, how it was disclosed and why it was disclosed.

5.3.10 The exception to this would be when relevant information is being shared with consent as part of the care and treatment being provided to the individual.

6 Sharing Information

6.1 Verbally

Staff will ensure:

- the receiver of the information is properly identified
- the receiver of the information understands their responsibility
- information is shared on a “need to know” basis only
- confidential conversations cannot be overheard by other individuals

6.2 By Telephone

Staff will ensure that:

- the recipient is properly identified and are sure they are talking to that recipient , it may be appropriate to take a main switchboard number to verify it independently and call back
- the receiver of the information understands their responsibility
- information is shared on a “need to know” basis only
- confidential conversations cannot be overheard by other service users, staff or members of the public

If a request is for service user or staff information

- Always check the identity of the caller
- Take a number, verify it independently and call back if necessary
- Check whether they are entitled to the information they require,

Remember that even the fact that a person may be a patient in the hospital, or a may be employed by the Care Trust, could be confidential. If in doubt, consult with your line manager or the Information Governance Team.
It is good practice to record what information has been shared and who that information was shared with together with the reason for sharing.

6.3 By Email

Email is not always a secure method of sending personal sensitive and/or confidential information unless encryption is used. If using email:

- Ensure email system is protected by a password, which is kept secure
- NHS Contact e-mail system to NHS e-mail system is encrypted, i.e. nhs.net address to nhs.net address is secure. Other domains that are secure with NHS mail are gsi.gov.uk; x.gsi.gov.uk; gse.gov.uk; gsx.gov.uk; police.uk; pnn.police.uk; cjsm.net; scn.gov.uk and gcsx.gov.uk. ……@nhs.net …@ ensure it is marked as NHS Confidential,
- ensure it is password protected
- send password details in a separate e-mail to the information
- only send on a “need to know” basis
- ensure information is kept to a minimum

6.4 **By Fax**

The use of fax transfer should be avoided whenever possible. Where it is unavoidable ensure that you:

- use a “safe haven” fax machine, i.e. a machine that is in a safe and secure environment
- phone the recipient to ensure that they are aware a confidential fax is about to be sent , send a fax covering sheet to confirm correct number, confirm that the individual will wait by the machine to collect the fax and notify the sender to confirm receipt.
- remove personal identifiable data from any information, unless you are faxing to a known secure and private area – so called Safe haven. To identify an individual you may use a key identifier, such as NHS number, social services number, unique pupil number, employee number
- mark the fax as ‘NHS Confidential’ or ‘NHS Protect’ as appropriate.
- if your fax machine stores numbers in memory, always check that the number held is correct and current before sending confidential information.
- ensure that the document is removed from the fax machine memory, if it has one.

6.5 **By Post – Internal or External**

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly e.g. ‘confidential’ or ‘Addressee Only’ as appropriate. Always address the envelope in full.

External mail must also observe these rules. Special care should be taken with personal information is sent in quantity, such as health records, or collections of service users records on paper, CD/DVD, or other portable media. These should be all be sent by Royal Mail “Special Delivery” or by a secure courier.

6.6 **Request for Personal Information to other Employees of the Care Trust**

Information on individuals should only be released on a “need to know” basis.

- Always check with the member of staff that they are who they say they are, such as checking ID badge
- Always check whether they are entitled to the information
- Don’t be bullied into giving out information

This applies not only to health & social care records but also to staff records. If in doubt, check with your line manager or the Information Governance Team.

6.7 **Requests for Personal Information by the Police, Solicitors and the Media**

6.7.1 All requests for personal and/or sensitive information by the police, should be accompanied with either the consent of the individual or by the Police providing a Section 29 form held by Police forces which allows limited proportionate disclosure without the individuals consent to assist with the investigation of crime & apprehension of offenders.

6.7.2 All media requests should be immediately directed to the Communications Team -Do not give out any information under any circumstances.

6.8 **Removing personal-identifiable/confidential information out of Trust Premises**

6.8.1 It is sometimes necessary for employees to take information away from their normal base, for example when visiting a client or working from home. Employees who need to do this should discuss the need with their line manager. If they agree the following must be considered:

- Ensure that there is a record of any paper files that are being taken. This record should include, when the files are taken, by whom, where they are going and when they will be returned. Further information can be found in the Records Management Procedure.

- Ensure that any personal/confidential information in paper form, for example care records, or electronic formats for example CDs/laptops/memory sticks, etc. are appropriately secured prior to them leaving the Care Trust's building such as encryption, sealed containers.6.8.3 Ensure that any personal/confidential information in paper form, for example care records, or electronic formats for example CDs/laptops/memory sticks, etc. are appropriately secured prior to them leaving the Care Trust's building such as encryption, sealed containers.

- Ensure that they are put in the boot of the car or carried on your person while being transported from work place to home or other work place. Personal identifiable information and/or confidential information should not be left in the car (even if it is out of sight) overnight.

- Whilst at home, employees have personal responsibility to ensure the records are kept secure and confidential. This means that other family members/friends/colleagues must not be able to see the content or outside folder of the records, or be able to access electronic records.

6.8.2 Further information can be found in the Home Working Information Governance Procedure which is available on iCare. Personal identifiable and/or confidential information must not be loaded onto personal computer (non-work).

6.8.3 When returning records back to work, this must be carried out securely and safety. Manual records should be logged back, with a signature of the person returning the file and the date it was returned.

6.8.4 For electronic records on CD/DVD, memory sticks, etc. must be virus checked before being loaded onto any of the Care Trust's systems. It is the employee's responsibility to ensure that they do not overwrite any information that may have been added to the file since it was downloaded. This is particularly relevant to word and excel type documents.

6.9 **Working in the Community**

6.9.1 Special care of personal identifiable data should be taken by Care Trust employees working in the community – for example when visiting service users in their homes.

6.9.2 Employees should only carry the minimum required personal identifiable data with them. However working practice may require that an employee visits several clients' homes between visits to their base. As such they may be required to carry several client care records with them.

6.9.3 When making a home visit, the health/social care professional should make a judgement of whether it is safer to leave other client's information locked in the boot of their car, or whether to take the records with them.

6.9.4 If any records, diaries which contain personal identifiable data, are taken into the home, then the records must not be left unattended unless they are in a safe and secure place.

6.9.5 If the records are left in the car, they should be locked in the boot when the car is unattended. If the car has an alarm then it should be activated.

6.9.6 Personal identifiable data, including diaries, worksheets, files and the media on which it is stored, i.e. laptop should never be left on view such as on a car seat or footwell when unattended and must never be left in a car overnight, or when the employee is off duty. This includes the bag/box in which the information may be held.

6.9.7 Community based services should have suitable procedures for ensuring the security and confidentiality of service user's records. These procedures may vary to meet the needs of each service and its users, but must comply with the requirements of the Data Protection Act (General Data Protection Regulation from May 2018) and the Common Law duty of confidentiality.

6.10 **Passwords & Pin Numbers**

6.10.1 Personal passwords issued to or created by employees should be regarded as confidential. Passwords should:

- not be shared with anyone, including IT Services

- not relate to the employee or the system being accessed
- be changed on a regular basis.
- contain letters numbers and/or special characters i.e. bar449; dh38zp; rocket$hip7
- be changed immediately if it has been disclosed
- be unique to the system, i.e. do not have one password for several systems

6.10.2 Smart cards provide access to certain systems, for example the Patient Demographic Service, it is therefore important that smart cards are kept safe, secure and for your own personal use at all times. PIN numbers should be kept confidential and not shared.

6.10.3 Any attempts to breach security and/or confidentiality should be reported immediately to the Line Manager and a Datix adverse incident report form completed.

6.10.4 A breach of security or breach of confidentiality may result in disciplinary action and be a breach of the Computer Misuse Act 1990 and/or Data Protection Act 1998 (General Data Protection Regulation from May 2018), which could lead to criminal action being taken against you.

6.11 **Abuse of Privilege**

6.11.1 It is strictly forbidden for employees to look at any information relating to their own family, friends or acquaintances unless they are directly involved in their care or treatment or with the employee's administration on behalf of the Trust.

6.11.2 Under no circumstance should employees use social networking sites, i.e. Facebook, Twitter

- to share personal identifiable information
- to communicate with service users
- to share any information relating to your job role

6.11.3 Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action. If you have any concerns about this issue please discuss with your line manager, Human Resources or the Information Governance Team.

6.12 **Security/Avoidance of Incidents**

6.12.1 Do not talk about individuals in public places or where you can be overheard. Be careful how you discuss clients/patients/staff in work environments, not all staff need to be aware of your discussions

6.12.2 Do not leave any health & social records, staff records or confidential information, including diaries, worksheets, etc. lying around unattended

6.12.3 Make sure that any computer screens, or other displays of information, cannot be seen by the general public, and ensure your workstation is secure when left unattended and logged out at the end of the working day.

6.12.4 Never leave confidential information of any kind in the car even if it is locked.

6.12.5 Do not access any records that you do not have a legitimate reason to do so.

7 Disposal of Personal Identifiable and/or Confidential Information

7.1 Before disposing of any personal identifiable and/or confidential information, please refer to the NHS Code of Practice for Records Management, Corporate Records Policy, and Corporate Health Records and discuss with the Trust Information Governance Lead.

7.2 When disposing of personal-identifiable and/or confidential information always use 'Confidential Waste' bins/shredders. Keep the waste in a secure place until it can be collected for secure disposal. Further information on the disposal of waste can be found in the Waste Management Policy which is available on the web site.

7.3 CD/DVDs containing personal-identifiable information and/or confidential information must either be securely destroyed – this can be arranged by contacting the IM Service Desk.

7.4 Files no longer required must be deleted from the Personal Computer.

7.5 Computer hard disks are disposed of by contacting the Informatics Dept (Informatics Mersey) via the service desk. These must not be sent via any postal route but must be collected and delivered.

8 Individual's Rights

8.1 Mersey Care NHS Foundation Trust recognises that individual's rights are particularly important in relation to handling of confidential personal information.

8.2 Under the Data Protection Act a person has the right of access to their records. Individuals have a further right to restrict access to their records. Further information can be found in the Data Protection Policy and/or the guide How We Use your Information.

8.3 We have a duty to inform individuals on what we do with their information and how we use it, see the Trust website and "How we use your information" leaflet on the Information Governance trust website page.

8.4 Under the Freedom of Information Act and the Environmental Information Regulations a person has the right to ask whether we hold information and if they may see it. We have a duty to advise them if we hold the information and to provide that information subject to certain conditions and exemptions. All Freedom of Information requests must be forwarded to the Communications Department for processing.

9 Training, Awareness, Advice & Support

9.1 The Information Governance Team will work with the Learning & Development Team and Divisions to ensure that appropriate training is part of the induction process and that all staff then complete the mandatory annual information governance update training.

9.2 Additional training will be provided to staff as and when appropriate to ensure awareness of confidentiality is available to staff.

9.3 Advice and support is available to all staff through the Information Governance pages on the Trust Information Governance web pages or by contacting the Information Governance Team.

10 Monitoring, Reporting, Auditing & Reviewing

10.1 The use of service user feedback questionnaires will be used to monitor staff's compliance to this Code of Practice and monitoring of complaints.

10.2 Breaches of confidentiality including data loss will be notified through the incident reporting procedure and Datix reporting system. Further information can be found in the Trust Adverse Incident Reporting Policy.

10.3 All breaches of confidentiality and data loss will be investigated and reported to the Information Governance Committee. Depending upon the severity of the incident the Caldicott Guardian, Senior Information Risk Owner and/or the Information Commissioners Office and Commissioners will be informed.

10.4 NHS Digtal will receive assurance on our standards around data protection/confidentiality through the submission of the annual Data Security & Protection Toolkit.

10.5 This Code of Practice will be reviewed at least every two years or earlier if learning and outcomes from incidents change best practice or changes to legislation occur, and/or guidance from the Department of Health, NHS Digital and/or the Information Commissioner.

10.6 The Minutes and a Chair's report of each meeting of the Joint Senior Risk Owner/Information Governance Committee will be presented to the Executive Committee for oversight.

11 References

Legislation

- Data Protection Act 2018
- EU Directive: General Data Protection Regulation
- Health & Social Care Act 2001
- Human Rights Act 1998
- Access to Health Records Act 1990

- NHS Act 1997
- National Audit Act 1983
- Crime and Disorder Act 1998
- Health Service (Control of Patient Information) Regulations 2002
- AIDS (Control) Act 1987
- NHS (Venereal Diseases) Regulations 1974
- NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
- Human Fertilisation and Embryology Act 1990
- European Convention on Human Rights
- Common law duty of confidentiality
- Mental Capacity Act 2005
- Disability Discrimination Act 1995
- Freedom of Information Act 2000

Professional Guidance

- NHS Code of Confidentiality (Confidentiality: NHS Code of Practice – 2003)
- GMC Guidance - Confidentiality: Protecting and Providing Information (April 2004)
- BMA - Confidentiality and disclosure of health information (1999)
- Caldicott Report on the Use of Patient Identifiable Information
- Caldicott 2 Report – To Share or not to Share (2013)
- National Data Guardians Review
- NHS Care Records Guarantee
- General Social Care Council Code of Practice
- Data Protection Policy
- EU Directive: General Data Protection Regulation
- Consent to Treatment Policy
- Information Management Policy
- Incident / Accident Reporting Policy
- Information Governance Policy

12 Distribution

12.1 Staff will be advised of this Code of Practice through the Trust's Staff Communication Team Brief and publication on the trust intranet via "Your News" communication bulletin.

12.2 Managers are responsible for ensuring that staff read and are aware of this Code of Practice.

12.3 This Code of Practice will be widely available to all staff and volunteers via their line manager and the Care Trust's website.

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: NHS Code of Practice)*	

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.**	

Equality and Human Rights Analysis

Title: IT10 Confidentiality & Data Sharing Policy
Area covered: Confidentiality and Data Sharing within Mersey Care NHS Foundation Trust

What are the intended outcomes of this work? *Include outline of objectives and function aims* To give guidance on Confidentiality and Data Sharing to all Trust staff, including volunteers and independent contractors to ensure that this document does not have any adverse equality or human rights implications.
Who will be affected? *e.g. staff, patients, service users etc.* Staff, Service Users

Evidence
What evidence have you considered? Document content with current legal and department of health codes of practice
Disability (including learning disability) Document states it is available in different formats upon request
Sex Not applicable
Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.* Not applicable
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.* Not applicable
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.* Not applicable
Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.* Not applicable
Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.* Not applicable
Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.* Not applicable
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.* Not applicable

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.* Not applicable
Cross Cutting *implications to more than 1 protected characteristic* Not applicable

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.*
Not applicable

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* Not applicable

Eliminate discrimination, harassment and victimisation

Not applicable

Advance equality of opportunity

Not applicable

Promote good relations between groups

Not applicable

What is the overall impact?

The assessment panel view is that there are no equality and human rights issues with the document

Addressing the impact on equalities

Not required

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.*

Not required

For the record

Name of persons who carried out this assessment:

Kate Greenwood **Reviewed by Gina Kelly & Linda Yell 8.3.16**
Jacquie Ruddick
Gina Kelly

Date assessment completed:

19 October 2011 **Reviewed: 8.3.16**

Name of responsible Director:

Jim Hughes

Date assessment was signed: 19 October 2011

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Co-ordination of implementation • How will the implementation plan be co-ordinated and by whom? *Clear co-ordination is essential to monitor and sustain progress against the implementation plan and resolve any further issues that may arise.*	• The implementation plan will be co-ordinated by the Information Governance Manager. The plan will include distribution of the policy in accordance with the guidance in Policy and Procedure for the Development, Ratification, Distribution and Reviewing Policies and Procedures.	July 2016
Engaging staff • Who is affected directly or indirectly by the policy? • Are the most influential staff involved in the implementation? *Engaging staff and developing strong working relationships will provide a solid foundation for changes to be made.*	• This policy is applicable to all staff working for, or with, Mersey Care NHS Foundation Trust (the trust).	
Involving service users and carers • Is there a need to provide information to service users and carers regarding this policy? • Are there service users, carers, representatives or local organisations who could contribute to the implementation? *Involving service users and carers will ensure that any actions taken are in the best interest of services users and carers and that they are better informed about their care.*	• There is no need to provide service users or carers a copy of this Policy however it will be available via the Trust website or copies will be provided upon request in different formats. • Service Users and Carers will not be involved in implementing the procedure.	

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Communicating • What are the key messages to communicate to the different stakeholders? • How will these messages be communicated? *Effective communication will ensure that all those affected by the policy are kept informed thus smoothing the way for any changes. Promoting achievements can also provide encouragement to those involved.*	• Key messages are: - That all staff must comply with current legislation outlined within the Data Protection Act 1998 (wef May 2018 General Data Protection Regulation) and the NHS Code of Confidentiality. • All staff will be able to access the policy via their manager or the Trust website.	
Training • What are the training needs related to this policy? • Are people available with the skills to deliver the training? *All stakeholders need time to reflect on what the policy means to their current practice and key groups may need specific training to be able to deliver the policy.*	• Completion of Trust Induction and Corporate Essential Training • Staff will receive information regarding DPA Act & their responsibilities prior to being provided with "live" access to the Clinical Information Systems. • Training will be on-line via the HSCIC national training tool and via the trust e.learning system.Training completion will be overseen by the Information Governance Manager and monitored by the Joint SIRO & IG Committee.	Annually

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Resources • Have the financial impacts of any changes been established? • Is it possible to set up processes to re-invest any savings? • Are other resources required to enable the implementation of the policy e.g. increased staffing, new documentation? *Identification of resource impacts is essential at the start of the process to ensure action can be taken to address issues which may arise at a later stage.*	• There are no additional financial implications arising from the implementation of this procedure.	
Securing and sustaining change • Have the likely barriers to change and realistic ways to overcome them been identified? • Who needs to change and how do you plan to approach them? • Have arrangements been made with service managers to enable staff to attend briefing and training sessions? • Are arrangements in place to ensure the induction of new staff reflects the policy? *Initial barriers to implementation need to be addressed as well as those that may affect the on-going success of the policy*	• Consideration of potential barriers was discussed during the development of the procedure.	

IMPLEMENTATION PLAN	Issues identified / Action to be taken	Time-Scale
Evaluating • What are the main changes in practice that should be seen from the policy? • How might these changes be evaluated? • How will lessons learnt from the implementation of this policy be fed back into the organisation? *Evaluating and demonstrating the benefits of new policy is essential to promote the achievements of those involved and justifying changes that have been made.*	• Increased awareness in respect of the Data Protection Act and staff's responsibilities to comply with this and the NHS Code of Confidentiality. • Annual completion of Information Governance training – audited as part of the Information Governance Toolkit compliance • Surveys will also be conducted with Service Users & staff to ensure they are aware of their rights & understand the legislation. The results of the surveys will be monitored and reviewed by the Information Governance Committee on an annual basis.	March annually
<u>Other considerations</u>		