NHS
Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: IM6
Issue number: 11

Information sharing (overarching) policy

Lead executive	Medical Director/ Caldicott Guardian – Medical Effectiveness & Education
Authors details	Information Governance Lead/Data Protection Officer 07785 518439

Type of document	Policy
Target audience	All CWP staff
Document purpose	To provide guidance to Trust staff in relation to when to undertake a Data Protection Impact Assessment and in what circumstances an information sharing agreement may be required. The document also contains a link to the register of the approved information sharing agreements.

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 06-Jul-20
Implementation date	06-Jul-20	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
CP3	Health records policy
GR17	Freedom of information (FOI) policy
IM7	Confidentiality policy
GR12	Media relations policy
IM10	Information governance policy
IM1	Information Communications Technology (ICT) Acceptable usage policy
CP40	Safeguarding children policy
CP63	Access to health records policy
SOP18	National Data Opt Out

Document change history	
What is different?	Added reference to Data Protection Act 2018 (UK) Updated reference to Information Governance Toolkit to Data Security & Protection Toolkit Section 3 added clarification of meaning of IG compliant organisation Section 3.4 changed basis for sharing from consent to sharing for direct care Section 3.7 added national data opt out information
Appendices / electronic forms	
What is the impact of change?	Minimal impact, policy updated to reflect changes in legislation

Training requirements	Yes - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of Information Governance & Data Protection Sub-Committee

Corporate services	Corporate representatives of Information Governance & Data Protection Sub-Committee
External agencies	None

Financial resource implications	None

External references
1. Access to Health Records Act 1990 (only for manual records of deceased patients) 2. Audit Commission Act 1998 3. Children's Act 1989 4. Common Law Duty of Confidence 5. Computer Misuse Act 1990 6. Copyright Designs and Patents Act 1988 7. Crime & Disorder Act 1998 8. Freedom of Information Act 2000 9. Health & Social Care Act 2001 10. Human Rights Act 1998 11. Medical Act 1983 12. Medical Act Amendment Order 2000 13. Mental Health Act 1983 14. NHS & Community Care Act 1990 15. Professional Performance Act 1995 16. Regulation of Investigatory Powers Act 2000 17. The Adoption Act 1976 18. The Criminal Justice Act 2003 19. The Health Act 1999 (section 31) 20. The Health and Social Care Act 2001 21. Health Service Circulars 22. HSC2002/3 LASSL2002/2 Implementing the Caldicott Standard into Social Care 23. Confidentiality: NHS Code of Practice November 2003 24. Record Retention Guidelines for Local Authorities (2003), Records Management Society of Great Britain August 2003 25. General Medical Council, 2004, Confidentiality: Protecting and Providing Information 26. Information Commissioner, 2002. Uses and Disclosure of Health Data 27. Consent Form template (Appendix 2-6) based on Hampshire Partnership Trust consent proforma 28. Acknowledgement and thanks are given to Susan Morra of Sussex HIS for allowing us to use her protocol as the basis for this document 29. Confidentiality: NHS Code of Practice Supplementary Guidance: Public Interest Disclosures 2010 30. ICO data sharing code of practice May 2011 31. Caldicott2 – Information: To share or not to share. 32. NHS England The Information Governance review, March 2013Practical Guidance on the sharing of information and information governance for all NHS organisations specifically for Prevent and the Channel process 33. General Data Protection Regulation 2016 34. Data Protection Act 2018 (UK)

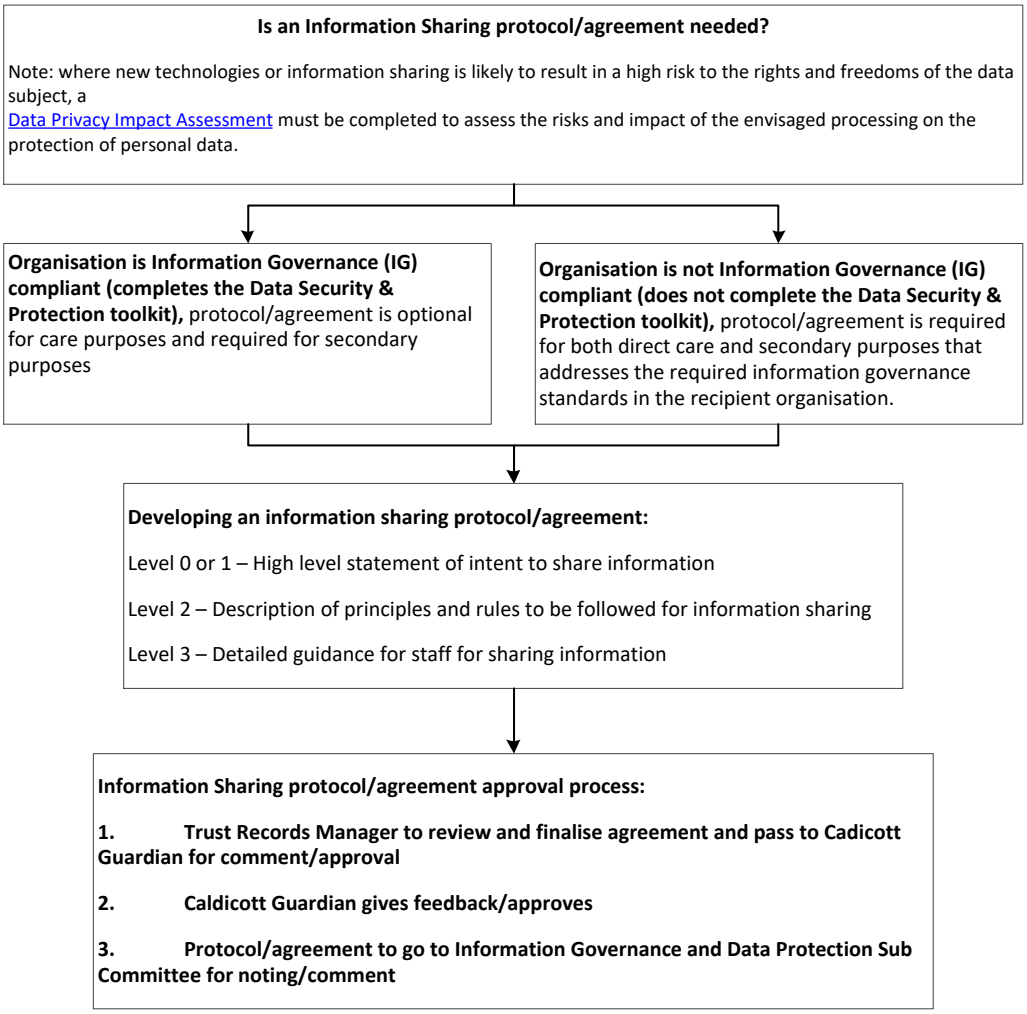
Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
No		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

Contents

Quick reference flowchart – Requisites for Information Sharing Protocol/Agreement

For quick reference the guide below is a summary of actions required.



1. Introduction

This policy outlines national and Cheshire and Wirral Partnership NHS Foundation Trust (CWP) standards for information sharing. Further advice on any aspect of the enclosed policy can be obtained from the Information Governance Lead/Data Protection Officer.

This overarching information sharing policy provides guidance for signed agreements between organisations that need to share person identifiable information. It sets out the obligations and commitments that staff must follow to ensure that legislation is not breached and patients' / clients' / families' / carers' / staff / employees' (collectively referred to as "service users" throughout this document) confidentiality is maintained.

This policy outlines the principles of confidentiality and establishes an interagency code of conduct with regard to the confidential management of service user's information.

Information sharing protocols can be a useful way of providing organisations with the boundaries of sharing information with other organisations. They can provide assurance in respect of the standards that each party to an agreement will adopt. However, they do not in themselves provide a lawful basis for sharing confidential information. That can only result from effectively informing the person whose information it is about the possibility of sharing and the choices they have to limit sharing. If the individual says no to sharing, then confidential information may only be shared in exceptional circumstances. It is consent that determines whether information can be shared - with consent you don't need an information sharing agreement for sharing to be lawful, without it an agreement is of no help.

Organisations will need to share confidential person-identifiable information with a range of others. The purposes of sharing information will either relate to the provision of care, including the quality assurance of that care, for the individual concerned or will be for non-care or secondary purposes, e.g. service evaluation, research, finance, public health work etc.

1.1 Objectives of policy

The objectives of this policy are:

- To provide a framework to clarify local procedures relating to the sharing of service user information;
- To ensure everyone working with personal information understands the importance of information sharing, where it improves care for service users and it is for the direct continuing care of service users;
- To ensure that only the minimum information necessary for the purpose should be shared;
- To ensure that when information needs to be shared, that sharing complies with the law, guidance and best practice;
- To ensure that service users' rights are respected;
- To ensure that confidentiality is adhered to unless there is a robust public interest in disclosure or a legal justification to do so;
- To outline the importance and benefits of information security and confidentiality training;
- To provide a mechanism for signatories to this policy to agree that their organisation and staff will comply with the standards and best practice for information sharing contained within this policy;
- To establish mechanisms for monitoring and audit of this policy.

2. Definitions

Data Security & Protection Toolkit (DSPT) – The toolkit is designed for organisations to demonstrate progress in implementing the 10 National Data Security Standards.

Tier 0 or 1 Overarching Agreement – This is a high level agreement to share information within the limits of law and guidance. This document is signed by the Chief Executive of participating organisations, or equivalent.

Tier 2 Information Sharing Arrangement – This sits under the Tier 1 and outlines the parameters for sharing, what is to be shared, the purposes and legal basis for sharing. This document is agreed and signed by the Caldicott Guardian in an NHS organisation or non-NHS equivalent. This document requires completion before it can be agreed as the specific purpose has to be included.

Tier 3 Operational Arrangement – This sits under the Tier 2 and describes the day to day operational processes that ensure the sharing is carried out to good governance standards.

Data Subject – A data subject is a person whom the data is about. Personal data is that which can identify, either directly or indirectly, a living individual.

Data Controller – A data controller is a person, or organisation, who determines the purposes for which and the manner in which any person data are to be processed.

Joint Data Controller - There can be more than one data controller for a data set. Joint controllers must clearly determine their respective responsibilities. They must ensure that there are appropriate contractual arrangements in place and to only use processors who can provide sufficient assurance that they will comply with data protection obligations.

Data Processor – Processing means storing, handling and processing of any kind of personal data. The term data processor is a legal definition of anyone other than an employee of the data controller who processes data on behalf of the data controller. Organisations who process personal data on behalf of another organisation e.g. payroll services are data processors. Employees of the data controller will process data but that does not make them under data protection law a data processor but they will be a data controller in their own right. This is why data protection is everyone's responsibility and knowing and reckless disregard can result in prosecution for the individual not just enforcement fines against the organisation.

Sensitive Data – Sensitive personal data is defined as:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs or trade union membership
- Processing of biometric or genetic data
- Health data
- Sexual orientation or sex life

3. Is a protocol required?

The below table sets out when a protocol is always required and when it is optional:

	Sharing for care purposes	Sharing for non-care purposes
Recipient organisation is achieving the required level of information governance performance e.g. completion of the data security & protection toolkit.	Sharing protocol is optional.	Sharing protocol necessary that focuses on the secondary uses in question, i.e. the purpose, constraints on re-use of information, retention periods and destruction policies.

Recipient organisation is unable to demonstrate the required information governance performance e.g. non-completion of the data security & protection toolkit.	Sharing protocol necessary that addresses the required information governance standards in the recipient organisation and the legal principles that apply.	Sharing protocol necessary that addresses the required information governance standards in the recipient organisation, the legal principles that apply and the additional standards associated with the secondary uses in question, (i.e. the purpose, constraints on re-use of information, retention periods and destruction).

There is a need to ensure that a protocol is always used when required. To provide this assurance there must be internal monitoring to ensure:

- Protocols are in place for all sharing with organisations that cannot demonstrate the required IG performance;
- Protocols are in place for all sharing for non-care purposes;
- That no new information sharing has begun without consideration of whether a protocol is required;
- That all staff with authority to share information with external partners are informed of and comply with the requirement to only do so within the framework of a sharing protocol (where one is required).

There should be periodic independent audit of recipients of information to ensure that the requirements of the sharing protocol are being adhered to.

3.1 Information sharing partners

Information partners will cover a range of organisation types, some of which will be 'trusted' organisations, whilst others will not. Organisations that can demonstrate they are attaining an acceptable level of information governance (IG) performance are those that are meeting the data security & protection toolkit key requirements. Some organisations are mandated to carry out IG assessments and ensure they reach an acceptable standard, such as other NHS organisations.

Others have a requirement to meet the key requirements because they are working with or for NHS organisations or have access to national NHS services and systems. This group will include some (but not all of) organisations such as:

- Social care services;
- Voluntary sector providers;
- Private sector care providers;
- Hospices;

Information sharing partners will also include organisations that have no current requirement to carry out IG assessments or do not provide IG assurance in the same way, such as:

- The police;
- Sure start teams;
- Education services;
- Housing services;
- Research organisations;
- The Department for Work and Pensions;
- Fire and rescue services;
- Youth offending teams;
- Court services;
- Probation services;
- The Crown Prosecution Service.

3.2 Data Protection Impact Assessments

Where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of processing, is likely to result in a high risk to the rights and freedoms of the data subject, a data protection impact assessment must be completed to assess the risks and impact of the envisaged processing on the protection of personal data. A template for completing a Data Protection Impact Assessment may be found on the Trust's information governance page of the intranet. Where the Trust cannot mitigate against significant risks, the Trust will be obliged to consult with the Information Commissioner's office prior to any processing of data.

3.3 Developing protocols

Information sharing protocols generally have three tiers or elements:

- A high level statement signed by the most senior member of the organisation, e.g. the Chief Executive, the Director of Adult Social Services, a partner / owner of a private sector care provider, etc and countersigned by the Caldicott Guardian (or equivalent senior person with responsibility for confidentiality) that binds the organisation into complying with the terms of the protocol;
- A description of the principles and rules that will be followed, consent procedures, legal compliance, security requirements etc;
- Guidance for staff on how to conduct day to day business with partner organisations who are party to the protocol.

Organisations that are meeting key IG requirements and have signed an IG assurance statement can be regarded as 'trusted' for information sharing purposes.

For these organisations the first two elements outlined above will be covered where the purpose is care delivery and will be largely covered for non-care purposes too. The third element, whilst not essential, is likely to be of value locally.

3.4 Sharing to provide care

In all circumstances there needs to be a strong IG management framework within the organisations that process confidential personal information. Many organisations, in particular in the NHS and social care are able to demonstrate that they have put the required IG framework in place by means of their Data Security & Protection Toolkit (DSPT) assessed performance.

Organisations that are achieving an adequate level of performance against the key DSPT requirements can be regarded as trusted organisations for information sharing purposes where the purpose of sharing is the delivery of care. These organisations will all be working to the same standards and will be taking appropriate action to satisfy legal requirements and hold information securely etc. Senior personnel in these organisations, e.g. NHS Chief Executives, Directors of Adult Social Services, sign an IG Assurance Statement (formerly an IG Statement of Compliance) to provide the required assurance to partner organisations.

Therefore, organisations are not required to put in place information sharing protocols where information sharing is between trusted organisations for care purposes. Such protocols may still be of value, however, where organisations feel that it is important to establish working procedures, contact points etc., that support day to day operational activity.

Where organisations are unable to demonstrate the required information governance performance to be classified as 'trusted', routine information sharing continues to require information sharing protocols in order to ensure that the 'rules' are clearly understood and that the requirements of law and guidance are being met. This is not to say that these organisations are failing to deliver effective information governance, rather that there is no agreed means for them to demonstrate that they are doing so in the absence of an agreed protocol, e.g. they are not mandated to complete the DS&P Toolkit.

In such situations, a protocol can also provide a useful and complete reference for the organisation of all the required actions to comply with the terms of the information sharing.

For clarity, an information sharing protocol is not required where the sharing is for an ad hoc request for information. Examples of such requests will include the following:

- When a service user moves house and registers to receive care from another organisation;
- Where a service user registered in one part of the country seeks emergency services from another;
- Where a service user is referred to a care provider outside of their catchment area for specialist treatment.

The basis for all these types of sharing would be sharing for direct care.

3.5 Sharing for non-care purposes

The approach where confidential personal information needs to be shared for non-care purposes needs to be managed somewhat differently even where the sharing is with a 'trusted' organisation. This is because the purposes for sharing need to be defined and limited, and additional requirements such as recorded informed consent or evidence of support under section 251 of the NHS Act 2006 (formerly section 60 of the Health & Social Care Act 2001), may be required to enable lawful sharing.

With 'trusted' organisations the required information sharing protocol only needs to focus on those aspects of sharing – purpose, constraints on re-use of information, retention periods and destruction policies – that are not normally associated with sharing for care purposes.

With other organisations, e.g. research or other secondary use organisations, the protocols will need to address both the basic information governance standards that should apply and the additional ones associated with the secondary uses in question – i.e. purpose, constraints on re-use of information, retention periods and destruction policies. See section 3.10 for information sharing protocols in place.

3.6 The NHS and Social Care Record Guarantees for England

Individuals' rights regarding the sharing of their personal information are supported by the **Care Record Guarantees**, which set out high-level commitments for protecting and safeguarding service user information, particularly in regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made. There are leaflets for service users on the CWP website at www.cwp.nhhs.uk which informs them of what information will be held about them, for what purpose, and in what circumstances the information may be shared. There are also leaflets for Learning Disabilities Patients `all about you'.

3.7 The National Data Opt Out

The national data opt-out allows a citizen to choose if they do not want their confidential health information to be used for purposes beyond their individual care and treatment - for research and planning. Citizens, or people acting for them by proxy, have control over setting or changing their own opt-out choice, and can change their mind at any time. If a citizen is aged 13 or over, they can set their own opt-out choice using the NHS digital online service, the NHS digital telephone service (0300 303 5678), the NHS App, or 'print-and-post' (www.nhs.uk/your-nhs-data-matters), completing an NHS digital form by hand and sending it into NHS digital. Someone can set an opt-out choice on behalf of a citizen, by proxy if: they are the parent or legal guardian of the citizen, who is a child aged 12 or under; they have a formal legal relationship with the individual, for example they have legal power of attorney or are a court-appointed deputy; They can only do this using the 'print and post' service. There are special arrangements for citizens in prison or other similar secure settings, known as

detained and secure estates. A health and care professional can help register a citizen's opt-out choice by filling in a proxy form available on the NHS digital website. All health and care organisations in England were required to comply with the national data opt-out policy by March 2020 (implementation date extended from March 2020 to September 2020 due to Coronavirus Covid19 pandemic):

- For direct care no action needs to be taken.
- Where the opt-out may apply e.g. research, the CWP Information Team has implemented a technical solution to enable NHS numbers to be checked with NHS digital to ensure that no information is used for citizens who have registered a national data opt-out preference
- The national data opt out standard operating procedure provides staff with guidance to ensure that the Trust complies with the national data opt-out policy.

3.8 Reporting breaches of the protocol

Inappropriate disclosures of information should be reported using the Trust on line DATIX incident form.

Any complaint received from a patient, service user, carer, voluntary organisation and / or public containing allegations of inappropriate disclosure of information will be dealt with through the complaints procedure of CWP and any other organisation who participated in the information sharing.

3.9 Agreement

Adoption of this overarching policy / agreement places an obligation upon the participating organisation to commit to a common best practice approach to confidentiality and sharing of person-based information. See Appendix 1 for list of information governance responsibilities which may guide organisations in identifying which areas of Information Governance may require more attention. The information sharing agreement in Appendix 2 is intended for organisations who are not subject to the NHS information governance requirements and who Cheshire and Wirral Partnership NHS Foundation Trust (CWP) intended to share person identifiable information with.

3.10 Procedure for Information sharing protocol approval

1. A Data Protection Impact Assessment must be completed for any processing which is likely to result in a high risk to the rights and freedoms of the data subject, to assess the risks and impact of the envisaged processing on the protection of personal data (see section 3.2).
2. Information sharing document either developed within or comes to the Trust from external source.
3. Information Governance Lead/Data Protection Officer reviews and passes comments to Caldicott Guardian.
4. Caldicott Guardian agrees or gives feedback in conjunction with relevant clinical management team if appropriate.
5. Information Governance Lead/Data Protection Officer ensures that document is noted on Information Governance & Data Protection Sub-Committee agenda, and any further comments passed back to Caldicott Guardian.

3.11 List of known local protocols or service level agreements / contracts

A register of all approved Information Sharing Agreements may be found on the information governance page of the Trust's intranet.

3.12 Consent template permission to share form

Staff may receive ad-hoc requests from an external source such as the police, the courts or the probation service. Sample consent forms may be found in the Confidentiality Policy

Appendix 1 Information governance areas which may require more attention

No	Responsibilities	Tick indicating compliance
1	Data Protection Notification to the Information Commissioner's Office is up to date.	☐
2	A Caldicott Guardian (or similar) is appointed.	☐
3	A Designated Officer (or similar) is appointed.	☐
4	Ensure the Caldicott Guardian (or similar), Designated Officer(s) (or similar) and the Data Protection Officer are widely known within the organisation and across signatory organisations. Use the list of signatory organisations below.	☐
5	Ensure that an information security policy is in place and that confidentiality and information security training is available to all staff including permanent, temporary, voluntary, contract, students on placements, locums, bank staff, etc.	☐
6	The organisation is aware that it will remain legally responsible for the information held within the organisation as required by data protection legislation.	☐
7	Ensure that the organisation you send information to is aware of the purpose for which the information was originally collected, and that processing does not contravene the General Data Protection Regulation 2016 and the Data Protection Act 2018. If an organisation needs to disclose the information it has received to yet another organisation it must always seek consent from the originating organisation before doing so.	☐
8	Agree to respond to requests for information within a reasonable time scale. (As agreed in local/specific protocols and included in legislation e.g. General Data Protection Regulation 2016/Data Protection Act 2018).	☐
9	All information sharing parties are issued with this inter-agency Code of Conduct.	☐
10	The organisation has signed confidentiality agreements for all staff, including permanent, temporary, voluntary, contract, students on placements, locums, bank staff etc.	☐
11	The organisation has confidentiality agreements with all contractors relating to service user information.	☐
12	Service user records are stored in appropriate secure lockable cabinets/rooms.	☐
13	Access to information is controlled (passwords and network access controls).	☐
14	There are clear audit trails for all accesses/uses of information.	☐
15	All information is backed up and backups are held in a fireproof safe.	☐
16	All backups held offsite are held securely and in fireproof safes if appropriate.	☐
17	All remote accesses to networks are provided by a secure virtual private network or similar.	☐
18	All information sharing is recorded for reasons other than for the direct continuing care of a service user.	☐

Appendix 2 Overarching information sharing agreement

This overarching information sharing agreement is intended for organisations who are not subject to the NHS information governance requirements and who Cheshire and Wirral Partnership NHS Foundation Trust (CWP) intended to share person identifiable information with.

Implementation of this agreement will require signatories to ensure that they recognise their responsibilities when sharing service user information and that there are appropriate processes in place in their organisation. These will include:

- Implementing and adhering to the procedures outlined in this document;
- Ensuring that all information sharing policies / procedures established between organisations / services are consistent;
- Training staff in the requirements of the policy;
- Informing service users about confidentiality;
- Allowing service users to access their records.

Compliance with this policy will be monitored by the Information Governance & Data Protection Sub-Committee, Cheshire and Wirral Partnership NHS Foundation Trust. The policy may also be monitored by any of the agencies who are signatories to this policy. This policy will be reviewed annually or sooner if legislation and guidance dictates.

Signatories:

Organisation	
Chief Executive	
Caldicott Guardian (or equivalent)	
Date	

On completion, this form must be returned to the Trust.

Note to Trust staff: upon receipt of completed agreement advise Information Governance Lead/Data Protection Officer

Appendix 3 Guidance for Trust staff - Questions and Answers

In most circumstances you should always act in the best interest of the service user and if in doubt talk to a relevant professional and/or designated officer, as you may need to also consider the interests of others such as carers, relatives, and other staff.

Q1. What if the service user is unable to read the leaflet due to sight impairment / illiteracy?
Answer - There is still a requirement to inform the service user. The information could be provided in larger font or different media e.g. audiotape, in Braille or verbally given by the professional to the service user. See section 3.6

Q2. What if the service user has difficulty in communication or language differences?
Answer - It is important to check for a clear and unambiguous signal of what is desired by the service user and to confirm the interpretation of that signal is correct by repeating back the apparent choice. Information leaflets could be made available in different languages or an interpreter sought to verbally share the information with the service user. Note: failure to do so could be an offence under the Disability Discrimination Act 1995 and may prevent consent from being gained. See section 3.6

Q3. How is capacity measured?
Answer - All adults are presumed to have legal capacity unless there is clear evidence to the contrary. See CWP mental health act policies.

Q4. What if the child does not have capacity?
Answer - If the child does not have capacity whoever has 'legal parental responsibility' would need to be consulted, if available. Sometimes it is not easy to establish who has parental responsibility; there could be joint responsibility between mother and father. It is important to check that any person making a request for a child's records where the child does not have capacity has proper authority. Ideally there should be notes in the child's record to any unusual arrangements. It is sometimes best to check all requests made for children's records with the Designated Officer and / or Caldicott Guardian. Also see CWP Access to Health Records Policy. In cases of child protection the child's guardian or person with parental responsibility (this may be the Court in some cases) will be noted in the child's 'Child Protection' file.

Q5. What if the child makes one decision and the person with legal parental responsibility makes the opposite decision?
Answer - It will depend if the child has the 'capacity to understand'. Any decisions made by a healthcare professional, where appropriate, must be made in the child's best interests.

Q6. What do I do if the service user refuses consent to share their information?
Answer - Explain the need to share to include what will be shared, why this needs to happen and to whom the information will be given. Explain how their care may be affected if the information is not shared. Let them know that their refusal to share will be recorded on their record with their reason. The service user should also be made aware that in certain circumstances their information can and will be shared without their consent e.g. if other legislation states disclosure must occur e.g. to notify a birth to the Registrar of Births, Marriages and Deaths or in circumstances where there is a legal obligation to share information in order to prevent crime or protect people. In some cases both staff and service user information has to be shared with others such as to the Audit Commission/NHS Counter Fraud employees for fraud investigation. See section 3.6

Q7. What if the complaint refers to a service user who has recently died and the record has details recorded by health and also social care staff. Can one of the organisations release the information recorded by the other?
Answer - In this case the General Data Protection Regulation 2016 does not apply as this only applies to information about living individuals. However, for health there is the 'Access to Health Records Act 1990' which allows relatives and those who may have a claim to have a copy of deceased patient records. See Access to Health Records Policy. There is no equivalent Act for Social Services and

advice should be sought from the relevant person as disclosure may or may not be allowed, dependent upon organisational policies.

Requests made to health organisations
All requests for access to records of deceased patients should be sent to the relevant health records department who will have an existing procedure for dealing with such requests. The request should be referred to the service user's last GP, where possible, or to another healthcare professional of equal standing to make any decision to release service user information. A fee may be chargeable and all requests must be dealt with within a predefined legal timescale.

Requests made to social care organisations
All requests should be directed to the relevant Designated Officer or Caldicott Guardian who will ensure the request is dealt with in the appropriate manner.

It should be noted that the Common Law duty of Confidence always applies. This means if the service user has stated that they do not want part or all of their record shared with their relatives when they have died this wish must be respected.

As a rule it is always best to seek further advice from the relevant records manager, Designated Officer, Caldicott Guardian or whoever deals with service user records.

Q8. What if a member of the public wish to record staff on the telephone, on Trust property or in public/person's home?
Answer - There are no legal grounds to prevent this from happening. Please refer to the Confidentiality Policy for detailed guidance.