



NORTHUMBERLAND AND NORTH TYNESIDE'S SAFEGUARDING ADULTS BOARD

MULTI-AGENCY INFORMATION SHARING POLICY

V1/April 2013

V2 October 2014

V3 March 15

Revision Date March 2016



CONTENTS

1. Introduction	3
2. Partners to Agreement	4
3. Key Legislation and Guidance	5
4. The Purpose of Information Sharing	6
5. Information which can be shared	6
6. Service User Privacy & Confidentiality	7
7. Sharing Confidential Information	8
8. Service User Consent	9
9. Service User Consent not Attainable	10
10. Service User Rights & Awareness	11
11. Information Sharing Procedures & Processes	12
12. Security	14
13. Management of Policy	14
14. Complaints	15
Appendix 1: Information Sharing Flow Chart	16
Appendix 2: Consent Form	17
Appendix 3: Information Request Form	19
Appendix 4: Record of Disclosure	21
Appendix 5: Golden Rules for Sharing Information	22
Appendix 6: Information Sharing Agreement – Signature Sheet	23



SECTION 1: **INTRODUCTION**

1. Northumberland and North Tyneside's Safeguarding Adults Board are multi- agency partnership responsible for co-ordinating the implementation of the Care Act 2014 and its guidance in relation to the development and implementation of policies and procedures to protect adults at risks from abuse or neglect.
2. The Care Act's guidance, which replaces the government's 'No Secrets' guidance prescribes that there should be adult safeguarding policies and procedures to support the reduction or removal of safeguarding risks. These procedures may include channels of inter-agency communication and procedures for information sharing and decision making. This current guidance adheres to the principles set out in 2005 by the Association of Directors of Social Services (ADASS) guidance entitled 'Safeguarding Adults: A National Framework of Standards for Good Practice in Adult Protection Work.' This ADASS guidance stated that the multi-agency partnership should have "information sharing protocols between all partner agencies, and those contracted to provide services by them that cover all aspects of safeguarding adults work".
3. The purpose of this document is to provide a legal and policy framework to facilitate the legitimate inter-agency sharing of information to protect vulnerable adults from abuse.
4. Through practice and experience we know for multi-agency safeguarding adult's procedures to be effective personal information must be appropriately shared across agencies in order that all information is available to those making decisions about concerns of abuse or neglect. When there is a need to share personal and/or sensitive data to protect an adult at risk of harm, the specific reasons for sharing the information should be recorded, along with an explanation as to why it is relevant. The volume and detail of the information shared must always be sufficient but not excessive for the required purpose. Wherever possible, decisions to share information should be made with the appropriate level of support, and not in staff isolation.
5. The intention of this document is for it to illustrate good practice standards which all staff from partner agencies need to meet in order fulfil their duty of care with regard to the sharing of information for the purposes of responding to or preventing abuse /neglect of vulnerable adults.

SECTION 2: **PARTNERS TO THE AGREEMENT**

6. The information sharing agreement is between the following partners;

Northumberland SAB

Northumberland County Council (Adult and Children's Directorates)
Northumberland Clinical Commissioning Group/NHS England
North Tyneside Council Adult Social Care and Children's Services
Northumbria Healthcare NHS Foundation Trust
Northumberland Tyne and Wear NHS Foundation Trust
Northumbria Police
Northumbria Community Rehabilitation Company
National Probation Service
North east Ambulance Service
Learning First (formerly Spiral Skills) Advocacy Services
Victim Support, Northumbria Branch
Healthwatch Northumberland
Age UK

North Tyneside SAB

North Tyneside Council Adult Social Care
North Tyneside Clinical Commissioning Group (CCG)/ NHS England
Northumbria Police
North Tyneside Children's Safeguarding Board
North Tyneside Council Elected Members
North Tyneside Homes
Northumbria Healthcare NHS Foundation Trust
Northumberland Tyne and Wear NHS Foundation Trust
Northumbria Community Rehabilitation Company
National Probation Service
Tyne and Wear Fire Service
North East Ambulance Service
North Tyneside Coalition of Disabled People
North Tyneside Carers Centre
Care Quality Commission (CQC)

7. It is the responsibility of the aforementioned partners;
- a) To understand their duty of confidentiality, and their duty to share information where there is a concern that a vulnerable adult, a child or member of the public is at risk of suffering harm;
 - b) To ensure that the agreement is cascaded amongst their staff within their organisation and any other organisation with which it contracts to provide a service to vulnerable adults;
 - c) To make sure all members of staff should have access to, understand and adhere to the information sharing policy;

- d) To put into practice the policy within their own organisation;
- e) To reproduce copies of the policy so it is widely available to users, carers and members of the public;
- f) To monitor and review the implementation of the policy within their own organisation and other organisations it contracts with.

SECTION 3: **KEY LEGISLATION AND GUIDANCE**

- 8. The information shared under this agreement is regulated by;
 - a) The Care Act 2015 <http://www.legislation.gov.uk/ukpga/2014/23/contents/enacted>
 - b) The Data Protection Act 1998 <http://www.legislation.gov.uk/ukpga/1998/29>
 - c) The Human Rights Act 1998; <http://www.legislation.gov.uk/ukpga/1998/42>
 - d) The Mental Capacity Act 2005; <http://www.legislation.gov.uk/ukpga/2005/9>
 - e) Crime and Disorder Act 1998 <http://www.legislation.gov.uk/ukpga/1998/37>
 - f) Freedom of Information Act 2000; <http://www.legislation.gov.uk/ukpga/2000/36>
 - g) The Caldicott Principles
 - h) The common law duty of confidentiality
 - i) Information Sharing: Guidance for Practitioners & Managers – HM Government
- 9. Any information sharing carried out will be done so in accordance with the eight principles of the Data Protection Act 1998, which provide that data must be;
 - a) Processed fairly and lawfully;
 - b) Processed for specified purposes
 - c) Adequate, relevant and not excessive
 - d) Accurate and kept up to date
 - e) Not kept for longer than is necessary
 - f) Processed in accordance with the rights of data subjects
 - g) Protected by appropriate security (practical and organisational)
 - h) Not transferred outside the European Economic Area without adequate protection

These principles assist in ensuring that;

- a) The legal basis for the information sharing is established and that there is both a clear and legitimate purpose and need for the information to be shared;
- b) That personal and sensitive information is anonymised where possible to prevent any identification of any individual within the information;
- c) Where possible consent should be sought from a person when information is going to be shared about them (consent may not be sought or is overridden where there is sufficient public interest)
- d) Where a person lacks the capacity to consent to information being shared as per the Mental Capacity Act 2005 a best interests decision should be made;
- e) Where there is uncertainty about sharing information, advice should be sought from managers, legal advisors or Caldicott guardians;
- f) Information is shared appropriately and securely;
- g) Records are made when information is shared or requested

SECTION 4: **THE PURPOSE OF INFORMATION SHARING**

10. The overriding objective of sharing information within the safeguarding adults framework is to ensure that all of the relevant facts are made available to support decisions that promote the safety of vulnerable people, reduce risks or prevent abuse from occurring in both the present and in the future.
11. Below is a list (not exhaustive) of situations where information sharing within safeguarding adults work may arise;
 - a) To obtain advice about specific safeguarding adults situation or to establish grounds for progressing with safeguarding adults procedures;
 - b) To make a safeguarding alert;
 - c) To gain immediate protection for a person(s) through referral to another service(s);
 - d) To inform agencies who may need to take action against an alleged or known perpetrator(s) (this may include risks which are posed by members of the public, worker, volunteer or a service user);
 - e) To make a referral to agencies for the purposes of requesting or amending services to people at risk of abuse or to those suspected of perpetrating abuse;
 - f) To complete a criminal investigation, an employment investigation, a regulatory investigation, a risk assessment and management plan, Safeguarding Adult Reviews or any other investigation or review as part of the safeguarding adults process e.g. Domestic Homicide Reviews or Child Serious Case Reviews
 - g) To monitor and audit safeguarding adults work e.g. alerts, quality of outcomes, adherence to procedures;
 - h) To continue reviewing and developing multi-agency policies and procedures to safeguard vulnerable adults;
 - i) To deal with complaints, grievances and professional or administrative malpractice;
 - j) The review of the information sharing agreement may identify; other reasons for sharing information not included above; and that the above are still necessary to effectively safeguard vulnerable adults.

SECTION 5: **INFORMATION WHICH CAN BE SHARED**

12. This agreement primarily applies to the sharing of information about a vulnerable adult (s) where there is a concern they may have about to be or have been a victim of abuse or neglect, however this may involve the sharing of information about others in order to safeguard other vulnerable adults children or the general public.
13. The agreement concerns the following personal and/or sensitive information which can be shared for the purposes outlined in section 4 (above):
 - a) "Personal data" which can identify the alleged victim(s) or alleged perpetrator(s) of abuse or neglect e.g. Name; date of birth address, NI number, facial photographs, CCTV footage as well as descriptions or photographic records of unique scars, tattoos or other markings;

- b) "Sensitive data" about the alleged victim(s) or alleged perpetrator(s) of abuse or neglect e.g. gender, religion, ethnicity, trade union membership, sexual relationships and criminal proceedings etc.;
 - c) Reasons for the concerns and details of the alleged concerns e.g. the nature of the abuse, the location of abuse, and the levels of risk and urgency
 - d) Information regarding the physical and/ or mental health of the alleged victim(s) or alleged perpetrator(s) e.g. mental capacity or communication needs
 - e) Reports of any medical or social care assessments or examinations undertaken as part of the safeguarding adults procedures e.g. eligibility for community care, psychiatric assessment
 - f) Personal data which identifies professionals involved with the alleged victim(s) or alleged perpetrator(s)
 - g) Personal data which identifies other people who may be at risk e.g. via employment family service
 - h) Historical information held in records about the alleged victim(s) or alleged perpetrator(s) that may be relevant to the current safeguarding concern e.g. previous safeguarding alerts
 - i) Name and contact details of the alerter
 - j) Name of the employer or organisation if the concern relates to a paid worker or volunteer of a service provider
14. Anonymised information about people which has been aggregated or tabulated in a manner which prevents identification to occur can be shared without the consent of those involved. Care should however be taken to ensure that it should not be possible to identify individuals either directly or in summation. This can occur when anonymised information is combined with data from different sources which produces small numbers in sample or where traceable reference numbers are utilised
15. Non personal information e.g. information about organisations, resources/projects or information about people that has been taken to a level that is not about individuals there is a general presumption which states information will be shared unless there are exceptional reasons as to why it cannot be such as
- a) Commercial confidentiality;
 - b) Policy formulation (where a policy is under development and circulation would prejudice its development)
 - c) Legal prejudice and
 - d) Where information is marked protectively

SECTION 6: **SERVICE USER PRIVACY & CONFIDENTIALITY**

16. Where it is necessary to share information, this will be done in accordance with the Data Protection Act 1998 (DPA 98) where this applies and any other relevant legislation.
17. In order that information is shared fairly and vulnerable adults are safeguarded, the following principles should be adhered to :
- a) Information sharing decisions will be based on considerations of safety and well-being of the person and others;

- b) The legal basis or enabling power for the information sharing should be established and recorded
- c) The DPA 98 should not be used as a barrier to sharing information but as a framework to ensure that personal information is shared appropriately in accordance with the DP Principles and Conditions. Confidentiality should never be confused with secrecy; in some circumstances it will be necessary to share personal information with or without the persons consent; (see section 9)
- d) A person has a right to know why, what, how and with whom information will or could be shared with as part of the safeguarding adults process;
- e) Whenever information is shared for a purpose other than the protection of people under safeguarding adults procedures (e.g. review of procedures training) then all personal information with be anonymised;
- f) Where the information subject is deceased their confidentiality endures beyond death please see additional legal advice.

SECTION 7: **SHARING CONFIDENTIAL INFORMATION**

18. The fundamental principle upon which the sharing of information is based is that it should not be utilised for any purpose or reason other than that which the individual gave consent for, unless subsequent permission is sought.
19. The key principle is that any information confided should not be used for any other purpose or disclosed further except as originally understood by the confider or with their subsequent permission.
20. Specific Information Sharing Principles are as follows;
 - a) Must have Lawful Authority (i.e. the enabling power)
 - b) Must be necessary
 - c) Must be proportionate
 - d) Must need to know
 - e) Must be accountable
 - f) Must ensure the safety and security of the information shared
21. The duty imposed is not absolute in nature and the disclosure of confidential information can be justified where:
 - a) The information is not confidential in nature;
 - b) The individual to whom the duty of confidence is owed has expressly authorised the disclosure of the information;
 - c) Disclosure is required by a court of law
 - d) It is required by legislation or legal obligation
 - e) If there is a serious overriding public interest that the information relates to such as;
 - Prevention or detection of Crime
 - Danger to a person's life
 - Danger to other people
 - Danger to the community
 - Serious threat to others, including staff

- Serious infringement of the law
- Serious risk to the health of the person

SECTION EIGHT:

SERVICE USER CONSENT (please see appendix 2 for Consent Form)

22. Where the informed consent of an individual is given, information will be shared unless there is clear justification for proceeding without consent. Informed consent means that the person giving consent understands why the information needs to be shared, what information will be shared, who will see their information, what the information will be utilised for and any implications arising from sharing the information.
23. Consent can be expressed verbally, in writing, or another form of communication although written consent is best practice, please see appendix two for template consent form. This includes sharing information with family members, close relatives and friends.
24. Information will only be shared for a specific and lawful purpose as indicated above where appropriate consent has been sought and obtained. The following list of purposes (although not exhaustive) are deemed as justifiable for the transfer of personal information between partner agencies;
- a) To make certain that vulnerable adults are given the appropriate care and protection required to live a life free from abuse, harm or exploitation;
 - b) The completion of a robust assessment to determine whether a vulnerable adult is at risk or is likely to be at risk of serious harm so all relevant information can be evaluated and contribute towards the development of risk assessment and risk management plan;
 - c) To ensure where safeguarding issues have been identified or where there are concerns about the care or treatment of a vulnerable adult that appropriate, timely and robust action can be taken to protect individuals from further harm;
 - d) For the prevention and detection of crime and/or promotion of community cohesion and safety;
 - e) To allow organisations to work together at both strategic and operation levels to bring about service improvements, enhanced delivery and to take action which better meet the needs of those who use the services;
 - f) To monitor and protect public health and wellbeing;
 - g) To ensure compliance with legal responsibilities e.g. court orders;
 - h) To allow for the investigation of complaints actual/potential legal claims;
 - i) To support and contribute towards Safeguarding Adults Reviews;
 - j) To enable individual(s) or agency(ies) in carrying out their statutory duties;
 - k) To support the provision of quality local data at appropriate levels so that policy and practice is evidence led;
 - l) To support the planning and commissioning of more efficient easier access to services;
 - m) To support improvements to existing and new services
 - n) To manage, report and benchmark performance
 - o) To promote accountability to customers, stakeholders local residents and government
 - p) Statistical analysis for research and training
 - q) To enable better co-ordination in promoting and marketing public events across the borough

25. There may be situations where individuals have a reasonable expectation that information may be shared without needing to obtain explicit consent (implied consent) such as where information is routinely shared and the individual is aware of this; or where the intrinsic purpose of providing the information is for it to be shared.
26. An individual may withdraw consent at any time, and when consent is being sought this must be explained to the individual. Where consent is withdrawn, all parties to whom the information has been should be notified immediately.
27. It is not best practice to assume that consent is open-ended, confirmation of consent should be re-sought after a reasonable period of time, taking into consideration the individual circumstances. It should be noted on the individuals file when consent has expired.
28. Where there are changes in circumstance such as the information needs to be shared with parties not involved when the initial consent was gained or where the extent of the information sought has changed, a revised consent should be sought, unless the information can be legitimately sought without consent.

SECTION NINE: **SERVICE USER CONSENT IS NOT ATTAINABLE**

29. Where it has not been possible to obtain consent prior to information being shared, the DPA 98 Schedule 2 and 3 conditions relevant to the sharing of the information should be established and recorded and the individual should be notified as soon as possible after the information has been disclosed, unless it is inappropriate to do so.
30. Where there is concern that a person lacks capacity to consent to information being shared, a capacity assessment will be completed as per the Mental Capacity Act 2005. If the assessment concludes that the person lacks capacity to consent, a best interest decision should be made, following the principles outlined in the Mental Capacity Act 2005.
31. When making a best interest decision regard should be had to the person's own views (where possible) and the views of those close to the person such as close relatives, partners, carers, welfare attorney's court-appointed deputies or guardians.
32. If a person has no-one to represent them or that person's representative is not seen to be acting the person's best interests or is the alleged perpetrator then an Independent Mental Capacity Advocate (IMCA) should be used where the decision relates to safeguarding adults procedures.

For the IMCA service in Northumberland please contact Learning First Advocacy Service on 0191 271 5353.

For IMCA service in North Tyneside please contact Your Voice Counts on 0191 4786472

33. Where a person makes a decision not to share information or a best interest decision is made where it is concluded that information should not be shared this decision should be respected where possible.
34. There will be some circumstances when consent will not be sought because it is unsafe, or where consent will be overridden (this should be determined on a case by case basis) such as ;
- if seeking consent would place a person (the individual, a family member or a third party) at increased risk of harm;
 - where seeking consent would prejudice the prevention detection or prosecution of a crime;
 - where it would lead to the unnecessary delay into making enquiries about concerns of significant harm to an adult at risk of harm or child;
 - where it is justified in the public interest this may include (to protect adults from serious harm; to protect children from serious harm; to prevent crime and disorder; in the interest of public safety). The question of whether there is sufficient public interest should be judged on the facts of each case. Where there is uncertainty whether the public interest justifies disclosing without consent, advice will be sought from a manager, designated lead person for safeguarding adults or the safeguarding adults team - where possible the identity of the person will not be disclosed;
 - Where a legal obligation has been imposed by the court or statute
35. Information will be shared about an alleged perpetrator without their consent where there is a reasonable belief that the sharing of information is necessary to protect a vulnerable adult or the wider public. A decision will be made at the strategy discussion/meeting about what and how information will be shared with an alleged perpetrator.
36. Where data needs to be shared in order to fulfill statutory requirements these requests will be considered and approved by the appropriate Caldicott Guardian, Data Protection Officer, Information Risk Officer, Freedom of Information Officer or those with similar responsibilities from the partner organisations.
37. If you are unsure about whether it is lawful to disclose information without consent, seek legal advice or contact your organisations Data Protection Officer or other designated officer as indicated above as this should **only be in exceptional circumstances**.

SECTION TEN: **SERVICE USER RIGHTS & AWARENESS**

38. All partners to this agreement will ensure that the information sharing policy is available to services users, carers and members of the general public. Partners have as responsibility to make service users aware of the purpose and content of this information sharing policy, it's impact upon them, their rights, and how these may be exercised
39. Information that is shared about a person will be kept on their records see appendix three for template and will normally be made available to that person and /or an appropriate representative. The right of access to information is made under the DPA 98. Requests should be made via subject access request.

40. When information is shared about a person they have the right to know the nature of the concerns, right to reply and an opportunity to correct any information regarding them which is inaccurate. This includes alleged perpetrators.
41. Exemptions to this right of access may be made if information identifies other people. Where this is the case there is the right to remove the information where there is concern that serious harm to the person or others would likely result if such disclosure to a third party occurred.
42. Where a person feels that their confidentiality has been breached they can make a complaint directly to the agency deemed responsible for that breach (see paragraph 61)

SECTION ELEVEN: **INFORMATION SHARING PROCEDURES AND PROCESSES**

Access

43. Partner organisations (to this policy listed in section 2), their contracted services and their respective staff or volunteers have access to information for those purposes outlined previously. It is the responsibility of those partner organisations to ensure there are procedures in place to ensure appropriate access to information by appropriate staff or volunteers.
44. Information will be stored and shared using secure methods which protect privacy and prevent risk of unauthorised access.

Methods of requesting & transferring information

45. This agreement applies to information that is shared in the following ways;

a) Verbally, face to face, in wider meetings

Verbal conversations and interviews should be recorded in a statement that is agreed by the information giver. Care must be taken to record and denote information clearly as fact, statement or opinion and to attribute any statement or opinion to the owner. All information should be recorded in such a way that it can be used as evidence in court should it be required at a later date.

b) Internal & External Post;

Internal mail should only be used for protect or unclassified information. With regards to external mail confidential and restricted information **must be sent via a secure delivery method** (e.g. recorded delivery or in person). Confidential or restricted information should be double enveloped, with no protective marking on the outer envelope only “to be opened by the named addressee only”. The outer envelope should also identify a return address. The inner envelope should be protectively marked as applicable.

c) Telephone;

When information is shared by telephone the giver of the information must verify that they are speaking to the intended recipient. Information will not be shared if it can be overheard by anyone who should not have access to it. A record should be made of the information given, to whom and how verified.

d) **Safeguarding adults meeting;**

When information is shared in a safeguarding adult meeting a confidentiality agreement will be signed by all present and this will be verbally highlighted as part of the agenda. All documents will be marked with a confidentiality clause stating "The contents of this document are restricted and should only be reproduced with the agreement of the Chair person; you are responsible for the safe storage and disposal of this document". Considerations should be made by the chair and all attendees for the sharing of third party information. Meetings should be recorded in minutes that are agreed by those present.

e) **Fax or Text phone;**

Information should be sent to fax/text phone numbers that have been verified as belonging to the intended recipient. The fax/text phone should be located in a safe and secure environment (safehaven). The person to whom the information is being sent should be notified that the information is about to be sent and that they will wait at the fax machine for the fax. Confirmation from the recipient to the originator should then be made that the information has been received.

f) **Email;**

Information will only be shared by email through a secure network or via encrypted email. Non-secure networks or non-encrypted email systems should never be used to send personal or sensitive information.

Some secure emails include;

- GSi (*.gsi.gov.uk)
- CJX (*.police.uk or .pnn.police.uk)
- GSE (*.gse.gov.uk)
- GCSX (*.gcsx.gov.uk)
- GSX (*.gsx.gov.uk)
- MoD (*.mod.uk)
- NHS *.nhs.net)

This is not an exhaustive list

g) **Databases/electronic records**

Information stored electronically will be used in accordance with agreed policies and guidance in relation to the recording of information, security of information and authorized access levels.

46. The safe and secure handling and transfer of information will depend upon the level of sensitivity of the information

47. All documents should be marked according to the protective marking scheme.
48. Recipients of information will understand the purpose for which the information was shared and the limits of any consent that has been given e.g. whether they are able to share the information further. Where this is uncertainty then the originating person/organisation should be contacted.
49. All decisions relating to information sharing, and the reason why the decision was made, will be recorded. This includes if a decision was made not to share information. Good practice examples for recording requests and responses to requests for information sharing appendix four

SECTION TWELVE: **SECURITY**

50. Partners to this agreement must implement and maintain appropriate security measures to protect confidentiality, integrity and availability of personal information.
51. Adopted security measures should be communicated across all partner organisations, their contracted services and their respected staff and volunteers.
52. Any organisation who is not party to this protocol but who wishes to share information may do so providing that there is an existing information sharing agreement in place with the third party that they agree to comply with the terms of this protocol and have adequate technical and non-technical security arrangements in place.

Data Retention, Review & Disposal

53. Information will be retained in line with the relevant organisations retention schedules
54. Staff should review individual cases files on a case by case basis, taking into account any outstanding subject access requests
55. When the retention period has expired, the information must be disposed of in a secure and safe way e.g. by using secure locked disposal bins or by using a cross cutting shredder
56. Please follow link to NCC Information Storage Policy –

<http://nww.northumbria.nhs.uk/home/wp-content/uploads/2012/04/Records-Management-Policy.pdf>

Please also refer to your own organisation's policy

SECTION THIRTEEN: **MANAGEMENT OF INFORMATION SHARING POLICY**

57. This information sharing agreement is owned by Northumberland and North Tyneside's Safeguarding Adults Boards



58. The Information Sharing Agreement will be signed by Northumberland and North Tyneside's Safeguarding Board Members on behalf of their organisations.
59. This agreement is effective from 1st April 2015.
60. The agreement will be reviewed every year to ensure that it is supporting Northumberland and North Tyneside's Safeguarding Adults Board in sharing information in a safe manner and is also having the desired effect of safeguarding vulnerable adults in Northumberland and North Tyneside.
61. Non-Compliance with this agreement will be referred to the Independent Chair of Northumberland or North Tyneside's Safeguarding Adults Board.

SECTION FOURTEEN: **COMPLAINTS**

62. Partner organisations must have in place procedures to address complaints relating to disclosure of information. The partner organisations agree to co-operate in any complaint investigation where they have information that is relevant to the investigation. Partners must also ensure that their complaints procedures are well publicised.
63. If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers who should liaise to investigate the complaint.

APPENDIX ONE: INFORMATION SHARING FLOW CHART

Flowchart of key questions for information sharing

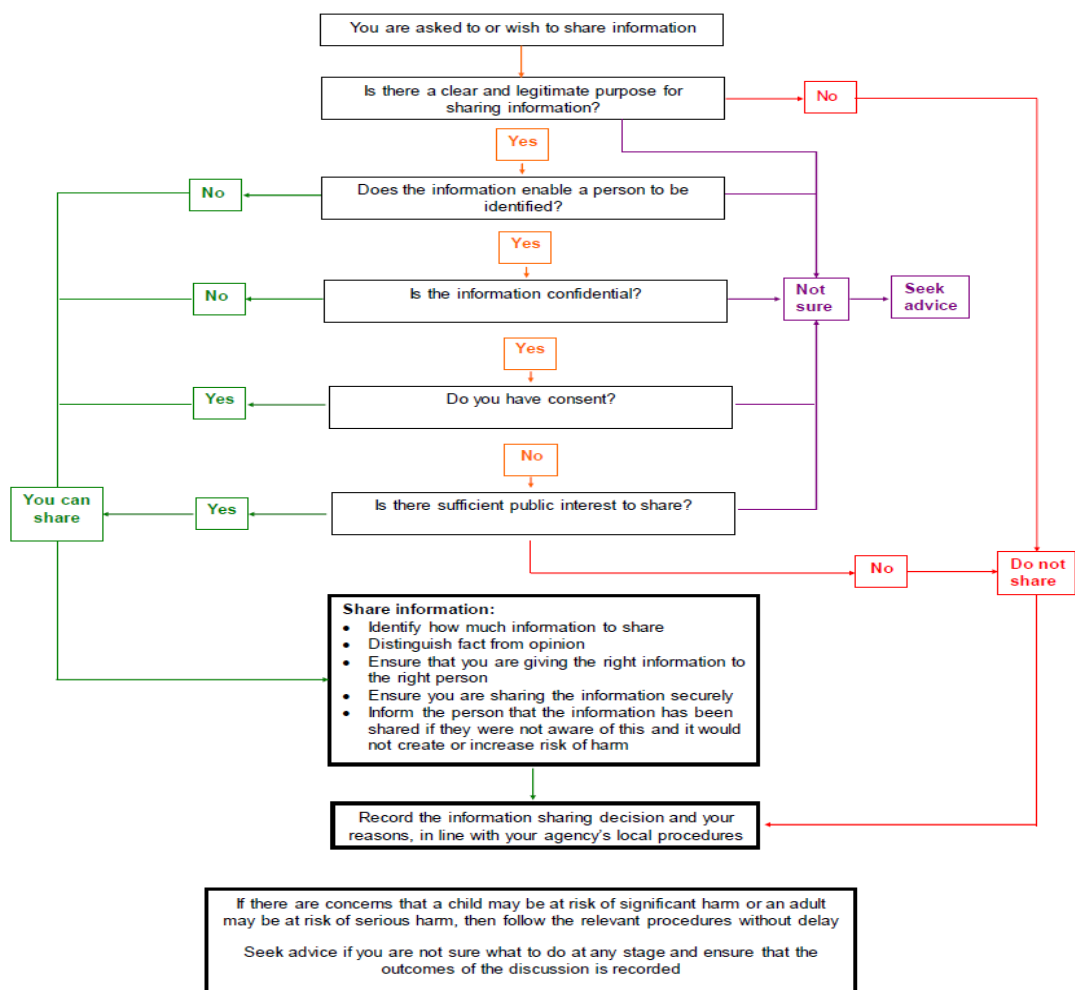


Diagram from: Information Sharing: Guidance for Practitioners & Managers HM Government

APPENDIX TWO – CONSENT FORM

INFORMATION SHARING POLICY – CONSENT FORM

Only to be used if no other consent documentation is available

Please complete the following;

Does this information concern you?	Yes No (please circle as appropriate)
If your answer is 'no' who is the information regarding?	
Name	
Address	
Date of Birth	
Are you acting as?	Parent / Guardian / Carer / Other (please specify)

Have the reasons for requesting your consent for information to be shared been explained to you?	Yes No (please circle as appropriate)
--	---

Statement of Consent

I _____ of _____

give my consent to _____ to disclose and share information



as detailed below to _____

Details of the information to which this consent applies

--

If you answered 'no' please complete the following;

Name	
Address	
Date of Birth	

Signed: _____

Print Name: _____

Dated: _____

Witnessed by:

Signed: _____

Print Name: _____

Dated: _____



APPENDIX THREE REQUEST/DISCLOSURE FORM

Part A – Information Requested (to be completed by the individual requesting information)

Individual Requesting Information:

Name	
Organisation:	
Telephone Number:	
Email Address:	

Information Requested:

--

Why is this information requested?

--

Date information is required by? _____

If the request is urgent please explain why:

--

Has Consent been obtained?	Yes No (please circle as appropriate)
----------------------------	---

If consent has not been obtained please tick the appropriate box below as to why this information is required?

Preventing serious harm to an adult - This may include prevention, detection and prosecution of a crime	
Providing urgent medical treatment to an adult	
Implementing the Department of Health's 'No Secret Agenda' - Which aims to protect vulnerable adults from abuse	
In the 'public interest' and a 'legitimate purpose to share' - See section ?? of the information sharing protocol	
There is statutory obligation or court order to share	

Signature of individual requesting information:

Dated:

APPENDIX FOUR – RECORD OF DISCLOSURE FORM

CONFIDENTIAL RECORD OF DISCLOSURE

Service User Name	
Service User Date of Birth	
Swift Number	
NHS Number (if relevant)	
Description of Data Disclosed	
Reason for Disclosure	
Recipient of Data	
If disclosed without consent, please state reasons	
Reasons for refusal/limited disclosure (if appropriate)	
Disclosing Organisation	
Disclosed by	

Authorised By	
Date of Disclosure	

A copy of this disclosure record should be retained on the service user's file
APPENDIX 5 – SEVEN GOLDEN RULES FOR SHARING INFORMATION
 (as per the HM Government Information sharing guidance for practitioners and managers)

Rule 1: The Data Protection Act 1998 is not a barrier to sharing information

The Data Protection Act 1998 provides a framework which ensures that personal information about living persons is shared appropriately.

Rule 2: Be Open and Honest

This is applicable to the person, and/or their family where appropriate from the outset about why, what, how, and with whom the information will or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

Rule 3: Seek Advice

If you are in doubt, without disclosing the identity of the person where possible.

Rule 4: Share with consent where appropriate...

And where possible respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgment, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

Rule 5: Consider Safety and Well-Being

Base your information sharing decisions on considerations of the safety and will-being of the person and others who may be affected by their actions.

Rule 6: Necessary, Proportionate, relevant, accurate, timely and secure

Ensure that the information you share is necessary for the purpose which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion and is shared securely.

Rule 7: Keep a record

Of all your decisions and the reasons for them – whether it is to share information or not. If you decide to share, then record what you have shared with whom and for what purpose.



APPENDIX 6 - INFORMATION SHARING AGREEMENT – SIGNATURE SHEET

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	



Date:	
-------	--

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration	



Date Renewal:	
---------------	--

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	



Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	



--	--

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	



Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	



--	--

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

--	--

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration Date Renewal:	

Signed by, for and on behalf of:

Organisation:	
Name:	
Position:	
Contact details; i.e. Phone No: E-mail:	
Signature:	
Date:	

Organisation Contact for Information Sharing:	
Position:	
Contact details; i.e. Phone No: E-mail:	
(DPA98) Registration Number	
(DPA98) Registration	



Date Renewal:	
---------------	--