NCASP

NORTHUMBERLAND CHILDREN AND ADULTS SAFEGUARDING PARTNERSHIP

Information Sharing Protocol

for practitioners working with children and adults with needs for care and support

NORTHUMBRIA POLICE

NHS

North East and North Cumbria

Northumberland County Council

Version Control

Title	**Information Sharing Protocol for Practitioners Working with Children and Adults**
Version	V3.04.24
Date	April 2024
Author	Northumberland Children and Adults Safeguarding Partnership

Update and Approval Process			
Version	Group/Person	Date	Comments
V1.12.22	NCASP – Business Manager	December 2022	Reviewed and adapted from Gateshead ISP
V2.02.24	NCASP – Business Manager	February 2024	Reviewed and updated following revised statutory guidance (WT2023)
V3.04.24	NCASP – Business Manager	April 2024	Reviewed and updated following revised guidance (information sharing for people who provide safeguarding services to children, young people, parents and carers)

Issue date	**April 2024**
Review date	**April 2025**

Contents

1. INTRODUCTION

Effective and legally compliant sharing of information between practitioners and local organisations is essential for early identification of need, assessment and service provision to safeguard children and adults with needs for care and support.

Case Reviews have consistently highlighted that missed opportunities to record, understand the significance of and share information in a timely manner can have serious consequences for the safety and welfare of children and adults at risk.

Northumberland Children and Adults Safeguarding Partnership (NCASP) delivers an integrated and joined up service which embraces the "Think Family" approach. It is essential that collaborative working and good information sharing is established throughout agencies, at all levels, which is then embedded through effective safeguarding practice.

This protocol has been developed to address information sharing both at strategic level and operational level within the arenas of Safeguarding Children and Adult Safeguarding. It is intended that agencies with the potential to be involved in safeguarding investigations will sign up to the use of this protocol.

This protocol is agreed with the purpose of ensuring compliance with the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 and the Human Rights Act 1998.

This protocol will be underpinned by *service specific operational agreements* that are designed to meet the specific data sharing needs of that service.

2. PURPOSE

This protocol has been developed to:

promote effective multi-agency working to support the work of all providers across Northumberland and to ensure the safety and promote the welfare of children and adults with needs for care and support.

ensure legislation and government guidelines are followed for effective and lawful sharing of information by all practitioners.

This document should be read in conjunction with:
Northumberland Multi-Agency Safeguarding Children Procedures and Multi-Agency Safeguarding Adults procedures.

The National Police Chiefs Council (NPCC) has also developed guidance: MASH Advice to Police Forces on Information Sharing for Child Safeguarding (to go with their Data Sharing 'Share With Confidence' guidance and flowchart)

Effective communication and information sharing is essential to safeguarding children and adults with needs for care and support.

Working Together to Safeguard Children 2023 Statutory Guidance (chapter 1: Information Sharing) stresses the importance of effective sharing of information between practitioners, local organisations and agencies to keep children safe and states practitioners should be proactive in sharing information as early as possible to help identify, assess, and respond to risks or concerns about the safety and welfare of children. Rapid reviews and child safeguarding practice reviews have highlighted that missed opportunities to record, understand the significance of, and share information in a timely manner can have severe consequences for children.

The Care Act 2014 envisages organisations sharing information in a safeguarding context to allow local authorities to enquire whether action should be taken to safeguard adults with needs for care and support who are at risk of abuse or neglect. It also sets out a *'duty to cooperate'* between the local authority and relevant partner organisations in relation to their Care Act responsibilities. This may be relevant in terms of sharing information where there are safeguarding concerns. The legislation emphasises the need to empower people, to balance choice and control for individuals against preventing harm and reducing risk, and to respond proportionately to safeguarding concerns.

Early sharing of information is the key to providing effective early help where there are emerging problems. Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of children and adults.

The seventh Caldicott principle states: *The duty to share information can be as important as the duty to protect patient confidentiality.* Professional duty of care is now seen to encompass both adults and children who are vulnerable not just to harm but also to their welfare being adversely affected without the provision of services.

To ensure effective safeguarding arrangements:

All organisations	Practitioners
• should have arrangements in place which set out clearly the processes and the principles for sharing information internally. •In addition, these arrangements should cover sharing information with other organisations and practitioners, including third party providers.	•should not assume that someone else will pass on information which they think may be critical to keeping a child or adult safe. •If a practitioner has concerns about a child or an adult's welfare and believes they are suffering or likely to suffer harm, then information should be shared with the relevant Social Care Team and/or the Police. •Practitioners should be particularly alert to the importance of sharing information when a child or adult moves from one local authority area to another.

3. WHAT IS INFORMATION SHARING?

Information sharing should take place in circumstances where there is a ***clear need*** for the exchange of information to take place and there are ***legal powers*** which permit agencies to do so. The information shared should be ***relevant and proportionate*** to the purpose concerned.

Information sharing can take place in a number of ways:

Disclosure:	Pooling:	Exchange:	Reporting:
•an agency acknowledges that it possesses relevant data. •It may make that data accessible to a requesting agency or individual but retains ownership and responsibility.	•in which agencies pool available data and maintain single service- based records.	•in which one agency provides one or more other agencies with relevant data. •Ownership and responsibility passes to the new agency which may amend or update the record to meet further requirements.	•an agency provides statistical data for an agreed reporting mechanism which may be reported to local and national groups.

There are three types of information public sector agencies manage, and may share:

Organisational material plans, policies, guidelines, minutes of meetings.	**Statistical material** aggregated or anonymised data including relevant analysis.	**Personal data** - (as defined by the Data Protection Act 2018) is:
•This is generally freely available or can be made available under the requirements of the *Freedom of Information Act 2000* (subject to specific exemptions where the material concerned can be considered commercially sensitive or otherwise exempt from disclosure.) •However, NCASP are currently exempt from the FOI legislation and are not legally required to respond to requests for information. •Public authorities which make up the partnership are subject to the Freedom of Information Act 2000 and have their own procedures for responding to FOI requests.	•Exchange often involves the provision of raw data sets which the receiving agency may combine with other data to provide more detailed analysis. •This kind of data is usually structured to avoid the identification of specific individuals.	•any information which may identify a living individual, whether that individual is a service user, an employee or any other relevant person; •*for example, a name, address, customer reference number, photograph or CCTV image* •Any information which can clearly identify a living individual when combined with any other data. •Aggregate information which may contain information about a group of individuals from which a single individual can be identified.

4. LAWFUL BASIS FOR INFORMATION SHARING

When deciding whether to share personal data for the purpose of safeguarding adults or children, practitioners must first establish whether there is a lawful basis to share the information.

The four main areas of law that relate to the disclosure and sharing of information are:

The Common Law Duty of Confidentiality	The Human Rights Act 1998	UK General Data Protection Regulations (UK GDPR)	The Data Protection Act 2018

Article 8 of the European Convention on Human Rights gives everyone a right to respect for family life, home and correspondence. Authorities can only interfere with these rights if the practitioner is acting ***lawfully*** and pursuing a ***legitimate aim*** (including the protection of health and the rights of others) and the action is ***no more than is needed***.

The implementation of the Data Protection Act 2018 and UK GDPR incorporates the processing of personal data for safeguarding purposes within organisations. This includes *special category data* which relates to personal information of subjects which is especially sensitive and personal, (as defined at Article 4 of the UK GDPR) the exposure of which could significantly impact the rights and freedoms of data subjects. It also incorporates the processing of 'Criminal Offence Data' (as defined at section 11(2) of the DPA 2018), which includes data relating to the suspicion or allegation of an offence.

Each organisation is responsible for determining its lawful basis for processing of personal data. Where processing relates to Special Category and/or Criminal Offence Data, additional lawful bases will need to be identified.

Irrespective of what kind of personal data processing is in question, a lawful basis under UK GDPR Article 6 will always be required. All UK GDPR Article 6 bases provide an equal legitimate basis for processing personal data. This Protocol discusses where it may be appropriate to rely on Article 6(1)(a) 'Consent' (which must be positive not passive, clear, demonstrable and freely given). In this context either of Article 6(1)(e) 'Public Task', or Article 6(1)(f) 'Legitimate Interests' may be alternative appropriate bases.

Where practitioners need to share special category data and/or criminal offence data, they should be aware that the Data Protection Act 2018 includes the ***'safeguarding of children and individuals at risk'*** [also ***'preventing or detecting unlawful acts'***] as processing conditions within Schedule 1 of the Act that allows practitioners to share information without consent and can be used for the purposes of:

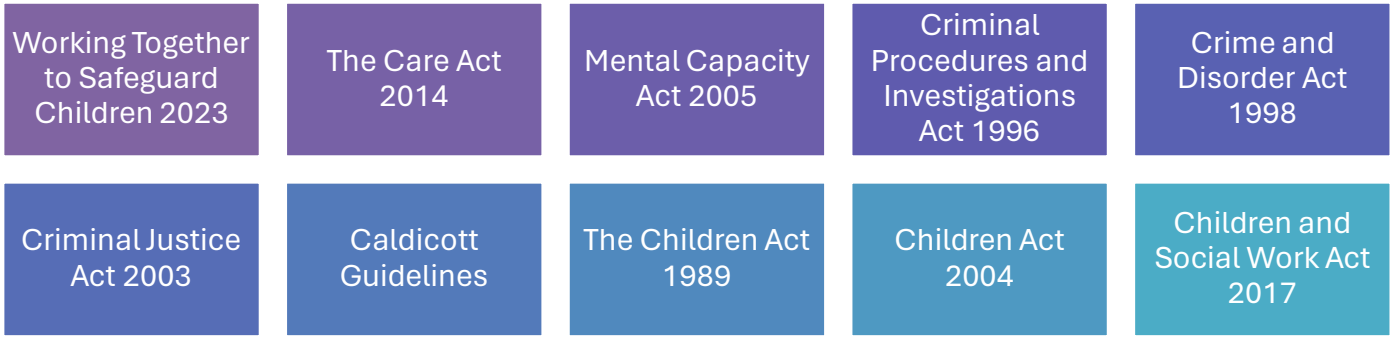
1. Protecting an individual from neglect or physical, mental or emotional harm
2. Protecting the physical, mental or emotional wellbeing of an individual

Specifically, this Protocol recognises the applicability of one or more of the 'Substantial Public Interest Conditions' at Part 2 to Schedule 1 of the DPA 2018 to processing of Special Category Data (and Criminal Offence Data) in this context, and which applies to both children and adults.

All information shared between agencies must have a ***defined and justifiable purpose*** and the information shared must be ***accurate and necessary*** for (and limited to) the purpose for which it is being shared; the information must be ***shared securely*** and shared ***only with those who need to see it***.

Safeguarding and promoting the safety and welfare of vulnerable children and adults with needs for care and support is the prime consideration in all decision making about sharing information.

Below is a list of the ***legislation*** and ***guidance*** that may need to be taken in consideration in the context of children's and adult safeguarding and information sharing:



Working Together to Safeguard Children 2023 requires the Statutory Safeguarding Partners to set out how they will work together and with any relevant agencies ensure that children are safeguarded and their welfare promoted. When selected by the Statutory Safeguarding Partners to be part of the local safeguarding arrangements relevant agencies must act in accordance with the arrangements.

The Statutory Safeguarding Partners can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act 2004 (as amended by the Children and Social Work Act 2017) for the purpose of enabling it to perform its functions.

The Care Act 2014 requires that the Statutory Safeguarding Partners establish Safeguarding Partnership arrangements to ensure that adults with needs for care and support are protected and their welfare is promoted. Each relevant partner must cooperate with the Safeguarding Partnership.

Section 45 of the Care Act 2014 relates to the '*supply of information*' and the responsibilities of others to comply with requests for information from the Safeguarding Adults Board in exercise of its functions.

The functions of NCASP include quality assurance practice involving joint audits of case files and case reviews involving practitioners for the purpose of identifying lessons learned. The legislation supports information sharing and allows for the multi-agency data to be shared for these purposes. Any request for information about individuals should be *necessary* and *proportionate* to the reason for the request.

In relation to multi-agency audits involving Primary Care a decision will be made on a case-by-case basis by the individual practice, based on General Medical Council guidance.

Any person may disclose information to a relevant authority under S 115 Crime and Disorder Act 1998 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)'. Relevant Authorities are the Police, Local authorities, Health Authorities (ICB) and the Probation Service.

5. INFORMATION RELATING TO A DECEASED PERSON

The UK GDPR and the Data Protection Act 2018 do not apply to deceased individuals. When considering disclosing information in relation to a deceased person the Common Law Duty of Confidentiality and the Human Rights Act 1998 must be considered, in addition to any other case-specific considerations.

6. THE PRINCIPLES OF INFORMATION SHARING

The Data Protection Act 2018 and UK GDPR are not barriers to collating and sharing information but provide a framework to ensure that personal information about living persons is shared lawfully and appropriately.

The Common Law Duty of Confidence and the Human Rights Act 1998 do not prevent the sharing of personal information. This can be because it is in the data subject's interests for the information to be disclosed or that public interest would justify the disclosure of the information.

The principles set out below are intended to help practitioners working with children, young people, adults with needs for care and support and parents and carers to share information between organisations:

Adequate

- Information should be adequate for its purpose.
- Information should be of the right quality to ensure that it can be understood and relied upon.

Relevant

- only information that is relevant to the purpose should be shared with those who need it.

Limited

- when taking decisions about what information to share practitioners should first consider how much information needs to be released.
- Only sharing data that is adequate, relevant and limited to what is necessary is a key principle of the UK GDPR and Data Protection Act 2018 and practitioners should consider the impact of disclosing information about the data subject and any third parties.
- Information must be proportionate to the need and level of risk.

Accurate

- information should be accurate and up to date and clearly distinguish between fact and opinion.
- Again, this is a key principle of the UK GDPR and Data Protection Act 2018.

Timely

- information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protect children and adults at risk.

Secure

- information should be shared securely and practitioners must always follow their organisation's policy on security for handling personal information.
- This is also a key principle of the UK GDPR and Data Protection Act 2018.

Record

- information sharing decisions should be recorded regardless of whether the decision is made to share or not.
- This record should include the rationale for the decision what information has been shared and with whom in line with organisational procedures.
- If the decision is not to share the reasons should be recorded.
- In line with each organisation's retention policy, the information should not be kept any longer than necessary. In some cases, this may be indefinitely.

Practitioners should use their judgement when making decisions about what information to share and should follow organisational procedures. The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child or adult including others who may be at risk.

See *Appendix 1* for the Seven Golden Rules of Information Sharing
See *Appendix 2* for an information sharing flowchart.

Remember that using professional curiosity can help to prevent risk. If there are concerns that a child or an adult may be at risk of serious harm, then practitioners have a duty to follow safeguarding procedures without delay. If a practitioner is uncertain about what to do at any stage, advice should be sought, and the outcome of the discussion should be recorded.

7. INFORMATION SHARING AND CONSENT IN SAFEGUARDING

Information which is relevant to safeguarding is often data which is considered to be 'special category data' meaning that it is sensitive and personal. The Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information without consent. In most genuine safeguarding cases it will be lawful to share information without consent.*

Consent does not need to be sought where the processing of people's personal data is based on any UK GDPR, Article 6 condition other than 6(1) (a) consent - for example the 'public task' condition or the legitimate interests condition and any UK GDPR, Article 9 condition other than 9(2)(a) 'explicit' consent.

[*Article 9(2)(g) of the UK GDPR provides for a Condition for lawful processing for 'Reasons of Substantial Public Interest (with a basis in law)'. Schedule 1 of the Data Protection Act 2018 includes (at section 18 within Part 2) 'safeguarding of children and individuals at risk' as a 'Substantial Public Interest Condition' that allows practitioners to share information further to identification of a lawful basis under Article 9, and without consent.]

Practitioners should proactively inform children and adults when they first engage with the service, about the organisation's policy on how information is shared and the lawful basis (Data Protection Act 2018/ UK GDPR) upon which their personal data is being processed.

Information may be shared *without consent* if a practitioner has reason to believe that there are grounds to do so, there is an identified lawful basis for doing so, and that the sharing of the information will enhance the safeguarding of the child or adult with needs for care and support in a timely manner and in their best interests.

Consent should not be sought from people who are not competent enough to provide consent – for example they are a very young child or have learning disability or difficulties that impact their understanding.

Consent should **not** be sought if doing so would:

- ❑ Place a person (the individual, family member, staff or a third party) at *increased risk of significant harm* (child) or *serious harm* (adult)

- ❑ Prejudice the prevention, detection or prosecution of a serious crime
- ❑ Lead to an unjustified delay in making enquiries about allegations of significant harm to a child or serious harm to an adult
- ❑ Demonstrate an imbalance of power – for example in a policing context**

**Consent is rarely sought in policing, as the Article 6 public task condition is applicable in most policing scenarios. [Information Commissioner's Office guidance discourages Local Authorities from relying on it.] Consent means giving people genuine choice and control over how an organisation use and share their data. Valid consent means people must be able to refuse consent to processing (e.g. sharing personal data) without detriment and must also be able to freely withdraw consent at any time.

The UK GDPR expressly states that where there is an imbalance of power between the parties in a business context/relationship, consent will not be a valid condition for using data, and so reliance on other applicable lawful bases for processing, both at Article 6 (the starting point for all Personal Data) and then Article 9 (essential to also have an Article 9 condition for processing Special Category Data), is necessary and important in order to assure compliance with the legislation.

When deciding whether to share confidential information the practitioner must judge on the facts of the case whether the sharing of the information is lawful, but also whether it is a necessary and proportionate response to the need to protect the child, the adult or the wider public from serious harm.

Sharing confidential information without consent will normally be justified in the public or vital interest when:

1. There is evidence or reasonable cause to believe a child is suffering or is at risk of suffering significant harm
2. To prevent significant harm to a child or serious harm to an adult including the wider public including through the prevention, detection and prosecution of a serious crime
3. Where there is an imbalance of power between the parties.

Where there is a clear risk of significant harm to a child or serious harm to adults, the public interest test will almost certainly be satisfied.

Consent should **not** be sought when there is a requirement by law to share information through a statutory duty or by a Court Order.

8. CALDICOTT PRINCIPLES

The Caldicott Principles and HM Government advice for practitioners on 7 Golden Rules are helpful in considering the justification for the sharing of information.

The Caldicott Principles were reviewed in April 2013 and the review found a strong consensus of support among practitioners and the public that the safe and appropriate sharing of information in the interests of the individual's direct care should be the rule not the exception, [although it will still always be necessary to identify a lawful basis for processing any personal data under the UK GDPR].

This coincided with a new Caldicott Principle:

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

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

9. SHARING INFORMATION APPROPRIATELY AND SECURELY

Practitioners must have due regard to the relevant data protection principles (at UK GDPR Article 5(1)) which allow them to share information appropriately and securely as outlined in the UK General Data Protection Regulation (UK GDPR) together with the Data Protection Act 2018, including UK GDPR Article 5(1)(f) ('integrity and confidentiality').

To share information effectively practitioners should:

Be confident of the conditions for lawful data processing under the Data Protection Act 2018 and UK GDPR

- This allows the storage and sharing of information for *safeguarding* purposes
- Including information which is *sensitive* and *personal* and should be treated as a '*special category personal data*'.

Be aware that the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition

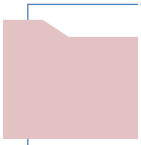
- This allows practitioners to share information.
- This includes allowing practitioners to share information in the interests of the individual at risk without their consent, where meeting the requisite threshold for consent (at Article 6) and explicit consent (at Article 9), is not possible, or would place a child or adult at risk.

10. METHODS OF REQUESTING AND TRANSFERRING INFORMATION

Wherever possible information shall be exchanged electronically by secure encrypted email. Information that cannot be exchanged by such means shall be transferred by other suitable methods that ensure the security and integrity of the information at all times.

11. SECURITY & STORAGE OF INFORMATION

Each signatory to this protocol:

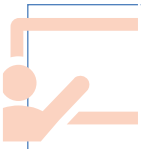


will ensure storage of all paper and electronic records adheres to the requirements of the UK GDPR & Data Protection Act 2018 and local and national information governance policy.

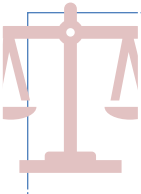
will ensure that all information is transmitted safely and securely in compliance with the UK GDPR & Data Protection Act 2018.

is responsible for protecting the personal and confidential data meeting the requirements of the UK GDPR & Data Protection Act 2018.

must have in place governance agreements which comply with the UK GDPR & Data Protection Act 2018.



must ensure all applicable staff complete Information Governance training, and abide by all aspects of data protection legislation and the Human Rights Act 1998.



will adhere to the common law duty of confidentiality.

12. INDIVIDUAL RIGHTS

Subject Access and other individual data rights under the UK GDPR/Data Protection Act 2018 – As Data Controllers, each organisation will follow its own procedures for data subject information rights and requests. Each organisation will consult where necessary with others, in relation to any source supplied personal data to establish any applicable non-disclosure exemption. This includes access to personal data, and the rights to rectify, object to data processing or erasure of personal data.

Personal data rights requests to the Safeguarding Partners, should be forwarded to Northumberland Council's Data Protection Officer: mark.eadington@northumberland.gov.uk

13. FREEDOM OF INFORMATION REQUESTS

NCASP is a statutory partnership and not a 'Public Authority' for the purposes of the Freedom of Information Act 2000. NCASP is therefore exempt from the statutory duty to provide information, although it will consider requests on an individual basis. **Individual organisations remain responsible for dealing with their own requests for information under the Act.**

In all instances **no** records of meetings will be **produced or shared** without the **express permission** of the Statutory Safeguarding Partners/Independent Scrutineer/Partnership Chair. All requests should be submitted to the Business Manager for NCASP – ncasp@northumberland.gov.uk

14. DATA BREACH INCIDENTS

Data protection related breaches or suspected breaches will be handled in accordance with the relevant provisions of the UK GDPR and associated ICO guidance, and NHS Digital guidance for reportable incidents and in accordance with the policies and procedures of each signatory organisation to this Protocol.

Any data breaches must be dealt with by the ***lead organisation*** in which the breach took place and reportable incidents must be reported to the ICO within 72 hours of the identified data breach. Where the data breach involves data from another partner organisation the investigating officer should inform and consult the relevant organisation at the earliest opportunity.

15. ADDITIONAL INFORMATION

Information Commissioner's Office (ICO)

- ❑ The ICO's *Data Sharing Code of Practice* and *Data Sharing Information Hub* provide detailed guidance, tools and other resources to aid data sharing in compliance with data protection law.
- ❑ *A 10 step guide to sharing information to safeguard children*
- ❑ *Lawful basis for processing*
- ❑ *Lawful basis interactive guidance tool*
- ❑ *A guide to lawful basis*
- ❑ *What are the conditions for processing?*

HM Government Information Sharing: Advice for Practitioners (2024)

- ❑ This *advice* is for practitioners and senior managers working with children, young people. It helps them decide when and how to share personal information legally and professionally.
- ❑ It might also be helpful for practitioners working with adults who are responsible for children who may be in need.

Working Together to Safeguard Children 2023

- ❑ This *statutory guidance* applies to all organisations and agencies who have functions relating to children (Chapter 1: A shared responsibility: *Information Sharing)*

National Police Chiefs' Council (NPCC)

- ❑ *MASH Advice to Police Forces on Information Sharing for Child Safeguarding provides* guidance *for those working within MASH (or similar).*
- ❑ Sits alongside their *Share with Confidence* Guidance

Keeping Children Safe in Education

- ❑ This is *statutory guidance* from the Department for Education.
- ❑ Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children (children includes everyone under the age of 18)

Child abuse concerns: guide for practitioners

- ❑ This *advice* is non-statutory, and has been produced to help practitioners identify child abuse and neglect and take appropriate action in response.

Care and support statutory guidance (issued under the Care Act 2014)

- ❑ *Statutory guidance* which outlines how local authorities should meet the legal obligations placed on them by the Care Act 2014 *and its accompanying regulations*

Care Act Factsheets

- ❑ These *factsheets* accompany Part 1 of the Care Act.
- ❑ *Factsheet 7: Protecting adults from abuse or neglect* - sets out how local authorities and other parts of the health and care system should protect adults at risk of abuse or neglect.

UK Caldicott Guardian Council

- *UKCGC* is the national body for Caldicott Guardians in the UK.
- Provides practical support, resources and networking opportunities for Caldicott Guardians and those fulfilling the Caldicott function within their organisations.
- UKCGC help people to uphold the eight Caldicott Principles.

Centre for Excellence on Information Sharing

- This *site* includes published resources produced over a four year programme supporting the public sector in overcoming information sharing challenges.

16. SIGNATORIES TO THIS PROTOCOL

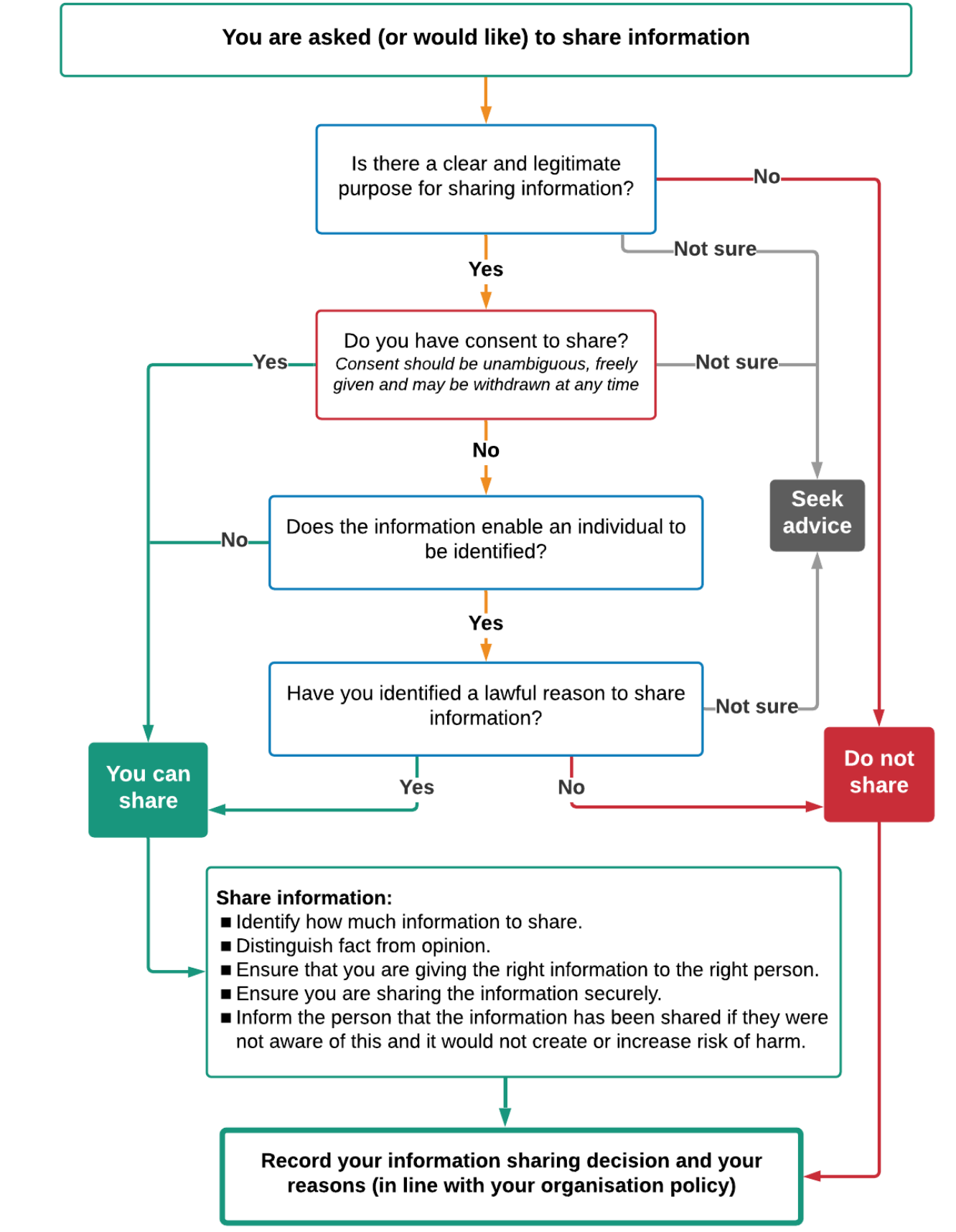
Statutory Safeguarding Partners (on behalf of NCASP including all Relevant Agencies)

Organisation	Position	Date
Northumberland County Council	Executive Director – Children, Young People and Education	29/02/2024
Northumberland County Council	Executive Director – Adults, Aging and Wellbeing	29/02/2024
North East North Cumbria ICB	Director of Nursing	29/02/2024
Northumbria Police	D/Chief Superintendent Safeguarding	29/02/2024

Appendix 1: Seven golden rules for information sharing

1	Remember that the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and human rights law are **not barriers** to justified information sharing. They provide a framework to support information sharing and ensure that personal information about living individuals is shared lawfully and appropriately.
2	**Be open and honest** with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3	Where possible, **share information with consent**, and where possible, **respect the wishes** of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information **without consent** if (in your judgement) there is a lawful basis to do so, such as where safety may be at risk. **You will need to base your judgement on the facts of the case.** When you are sharing or requesting personal information from someone, **be clear** of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.
4	**Seek advice promptly** from your manager/supervisor or your information governance lead if you are in any doubt about sharing the information concerned or do not understand how the legal framework supports information sharing in a particular case. ***Do not leave a child or adult at risk of harm because you have concerns you might be criticised for sharing information.***
5	**Consider safety and well-being:** base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions. Take steps to protect the identities of any individuals (e.g., the child, a carer, a neighbour, or a colleague) who might suffer harm if their details became known to an abuser or one of their associates.
6	**Necessary, proportionate, relevant, adequate, accurate, timely and secure:** Sharing information with a third party rarely requires you to share an entire record or case-file. Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7	**Keep a record of your decision and the reasons for it** – 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. Be willing to reconsider your decision if the requestor shares new information that might cause you to regard information you hold in a new light. When recording any decision, clearly set out the rationale and be prepared to explain your reasons if you are asked.

Appendix 2: Flowchart of when and how to share information



If there are concerns that a child is in need, suffering harm or likely to suffer harm or that adult with care and support needs is at risk of or experiencing abuse, follow the relevant procedure **without delay**.

Seek advice if unsure what to do at any stage and ensure that the outcome of the discussion is recorded.