D R A F T

Haringey Community Safety Partnership

Crime and Disorder Information Sharing Protocol

Revised document
March 2016

CONTENTS PAGE

List of Appendices

1. Introduction

1.1 It is the legal duty of all staff in statutory agencies, hereafter referred to as Partner Organisations, to share information for the purposes of preventing or detecting crime or disorder. This duty is set out in the terms of Section 115 of the Crime and Disorder Act. It is incumbent upon Community Safety Partnerships (CSP) to facilitate and promote information sharing and to update the protocols and processes which underpin it.

1.2 Since the last review, PREVENT work has become a duty and a separate information agreement has been signed to cover exchange of information in this context. The Clinical Commissioning Group (CCG), Community Rehabilitation Company (CRC) and Bridge Renewal Trust should all be new signatories. This Information Sharing Protocol (ISP) supersedes the previous version dated 2009.

1.3 This version strengthens the accountability and the role of CSP members who represent all Partner Organisations. This is outlined under section 7: Governance and Accountability.

1.4 It should, however, be noted that the absence of a protocol should not prevent sharing information. If you need to share information outside of the terms of this protocol or with agencies that are not party to this protocol you should follow the guidance as outlined in Haringey's *Simple Guide to Sharing Information,* appendix D.

1.5 This protocol ***must*** be read in conjunction with Appendix H: (HM Government guidance on information sharing for practitioners) and Appendix G: Information relating to children and parental consent.

The guiding rule remains:

If you need to share information in order to protect someone from harm or criminal activity, you must do so

2. Purpose of this protocol

2.1 The effective and timely sharing of information is essential to the delivery of high quality services focused on the needs of the individual and wider society. Effective sharing is also essential in many cases to the safeguarding of vulnerable individuals. In Haringey, we expect and encourage all professionals to share information with confidence as part of routine delivery.

2.2 Signatories to this protocol undertake to disclose and share informa-

tion for the purposes documented. This includes the provision of key data to inform partnership plans or joint tasking on an ongoing basis.

2.3 There are a number of IS agreements that sit beneath this protocol to address specific issues such as safeguarding, high risk case panels and the prevention of harm from extremism and radicalisation. It is also considered good practice to sign a simple confidentiality undertaking at the outset of individual case conferences. This protocol does not aim to capture all existing or future signed ISPs in the field and this is not considered to be necessary.

3 Legal basis regarding information exchange

3.1 The Crime & Disorder Act 1998 is the primary legislative tool, common to all crime reduction protocols. Section 17 of the Crime and Disorder Act 1998 (CDA1998) imposes a duty on the council to exercise its various functions with due regard to do all that it reasonably can to prevent, crime and disorder in its area. Section 115 of CDA1998 provides a general power, where it is necessary or expedient for the prevention of crime and disorder, to people/organisations without a power to disclose information to the authority, the power to do so.

3.2 The Data Protection Act 1998 places obligations on the owners of personal data to manage that data in accordance with 8 principles. The Act requires that the use of personal data, including information sharing, is fair, lawful and for specified purposes.

3.3 The Human Rights Act 1998 provides individuals with a right to respect for private and family life, free from unlawful and unnecessary intrusion by public authorities.

3.4 The Common Law Duty of Confidence applies to information provided to public authorities under an assumption or expectation of confidence.

3.5 Homelessness Act 2002 (HA2002) - Section 184 of the Housing Act 1996 allows the local authority (if it believes a person is homeless or threatened with homelessness) to make 'such enquiries as are necessary' to establish whether a person is eligible for housing assistance and what duty they are owed by the authority. This entitles relevant housing authorities to request information from the Metropolitan Police to establish the applicant's eligibility for housing assistance. Section 10 of the Homelessness Act 2002, extends the criteria for determining whether it is reasonable to continue to occupy accommodation to include those who have been made homeless as a result of being the subject of violence, or the threat of violence which is likely to be carried out.

3.6 There are other statutory provisions and guidance that permits local authorities and other organisations to share information for specific purposes, for example, to safeguard children and adults from abuse or neglect. Refer to Appendix G.

4. Types of information and rules about sharing it

Personal information

4.1 The Data Protection Act 1998 defines ‘personal information’ as information relating to a living individual who can be identified directly either from that information or from that information in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

4.2 A person’s full name is an obvious likely identifier; but other information such as a customer reference number, NINO, address, photographs or CCTV images could also identify them.

4.3 The definition of personal information is technology neutral; it does not matter how the information is stored (e.g. on a computer database, paper filing system, microfiche, portable memory stick).

4.4 Where it is necessary for information to be shared, personal information will be shared on a need-to-know basis with respect given to any duty of confidentiality.

4.5 Where the disclosure would breach client confidentiality the request should be referred to a designated manager - unless exceptional circumstances apply, e.g. where there is a need for urgent medical treatment. Managers should have access to a source of advice and support on information sharing issues. This may be a Caldicott Guardian.

4.6 The reasons for sharing confidential or personal information under these circumstances must be fully recorded and must clearly reference the evidence and information on which the decision is based. This must include details of any third parties and details of all the information/evidence they have been given

4.7 Examples of information that may be requested are:

- Demographics (name, date of birth, gender, address, ethnicity)
- Offending history
- Living Arrangements
- Family and personal relationships
- Statutory education
- Lifestyle and cultural factors
- Substance misuse
- Emotional and mental health
- Perceptions of self
- Thinking and behaviour
- Attitudes to engagement in relevant activity
- Motivation to change

Depersonalised information

4.8 Depersonalised information encompasses any information that does not and cannot be used to establish the identity of a living person, having had all identifiers removed.

4.8.1 Partner Organisations accept that there are no legal restrictions on the exchange of depersonalised information, although a duty of confidence may apply in certain circumstances, or a copyright, contractual or other legal restriction may prevent the information being disclosed to Partner Organisations.

4.8.2 Information shared between Partner Organisations should be limited for the purposes of the enquiry. If the purpose of this protocol can be achieved using depersonalised information, then this should be the preferred method used by officers. For example, in assessing crime hotspots geographic information that does not identify living individuals might be used for strategic planning purposes.

4.8.3 Partner Organisations recognise that care must be taken when depersonalising information and that the Information Commissioner has stated that even a post-code or address can reveal the identity of an individual. Partner Organisations are also aware that it may be possible for an individual's identity to be revealed by comparing several sets of depersonalised data.

4.8.4 The partners to this Protocol agree to share depersonalised information for all stated purposes and for use in annual strategic assessments and the purposes of joint tasking decisions. Examples of data sets are listed at appendix B. This is not an exhaustive list.

Non-personal information

4.8.5 Partner Organisations understand that non-personal information is information that does not, nor has ever, referred to individuals. Examples include recorded data by volume and trends; number of school exclusions; A&E hospital admissions. See appendix C.

5 Consent

5.1 Many issues surrounding the disclosure of personal information can be avoided if the consent of the individual has been sought and obtained. Obtaining consent remains a matter of good practice and in circumstances where it is appropriate and possible, informed consent should be sought. (There is a 'Consent Form' at appendix B of this protocol that can be used if signed consent has not already been obtained as part of the assessment or referral process). Consent lasts as long as required - unless it is withdrawn. Individuals have the right to withdraw consent after they have given it.

5.2 Practitioners should encourage clients to see information sharing (and giving their consent to share their personal information) in a positive light, as something which makes it easier for them to receive the services that they need.

6. Sharing information without consent

6.1 Practitioners should not seek consent when they are required by law to share information through a statutory duty or by a court order. Consent should also 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 if a child, or serious harm if an adult; or
- prejudice the prevention, detection or prosecution of a serious crime; or
- lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult.

6.2 There are many circumstances in which information shared under this protocol might be prejudiced if Partner Organisations were to seek consent. In such cases, the disclosing agency must consider the principle of 'legitimate purpose'. It is possible to disclose without consent if the issue is of substantial 'public interest' in which case any duty of confidentiality can be overridden.

Legitimate Purpose

6.3 Partner Organisations understand the 'Legitimate Purpose' criteria to include:

- Preventing significant harm to a child or serious harm to an adult;
- Providing urgent medical treatment to an individual
- Implementing any of the following Acts: Crime and Disorder Act 1998, Homelessness Act 2002, Housing Act 1985 & 1996 Act

Public Interest

6.4 Partner Organisations understand the 'Public Interest' criteria to include:

- Administration of justice
- Maintenance of public safety
- Apprehension of offenders
- Prevention of crime and disorder
- Detection of crime
- Protection of vulnerable members of the community

6.5 When considering whether disclosure is in the public interest, the rights and interests of the individual must be taken into account. A fair balance between the public interest and the rights of the individual must be ensured.

7 Governance and accountability

7.1 This ISP requires the Partner Organisations will be actively represented through the relevant CSP board members. These members commit to taking responsibility for the effective and secure exchange of information, reporting any blockages or problems to the CSP Executive or CSP Board.

7.2 Through the CSP board members, Partner Organisations undertake to proactively publicise the existence of this ISP and the importance of compliance for all staff. Partner Organisations will further ensure the compatibility of these arrangements with information governance protocols in their own organisations.

7.3 The CSP will ensure that a regular review is undertaken and will take responsibility for ensuring that breaches of protocol are dealt with promptly and effectively within their respective organisations.

7.4 Each Partner Organisation will allocate the day to day role of Information Single Point of Contact (SPOC) to a designated role within their organisation plus one back- up role. The SPOC within organisations will be responsible for providing guidance and support on this protocol. Board members will be responsible for ensuring compliance with the ISP and all auditing and monitoring arrangements.

8 Requesting Information under this protocol

8.1 Where there is reasonable cause to believe that an individual may be at risk of suffering significant harm or serious harm, staff should always consider referring their concerns to social services or to the local police force – in line with the local policies and procedures.

8.2 When in any doubt, staff must talk to a lead person either a safe-guarding professional; their manager, an experienced colleague or a Caldicott Guardian. Staff should try to protect the identity of the individual (wherever possible), until they have established a reasonable cause for their belief.

8.3 Staff Requesting Information

8.3.1 An officer requesting information from another Partner Organisation must submit the inquiry in writing and on the 'Request/Disclosure Form' attached to this protocol at Appendix B.

8.3.2 The request must specify what is required and the purpose for which it is being sought. Any personal details **must** also be transmitted in a secure way, for example, through **secure/or GCSX** account or as **a password protected** document. It is not acceptable for any personal or detailed information to be circulated via the ordinary email route as this is inherently insecure and may breach the Data Protection Act.

8.3.3 The requesting officer must also save a copy of the request on the client's record.

8.3.4 There is no need to submit a separate form for each occurrence. The procedure is subject to a continued review by participating Partner Organisations.

9 Disclosing Information under this protocol

9.1 Officers responding to a request for information must consider the safety and welfare of the client when making decisions on whether to share information about them.

9.2 The disclosing officer must ensure that the requesting officer has supplied a complete 'Request/Disclosure' form and, where appropriate, evidence of the client's consent. A reply to the request must be made within an agreed timescale.

9.3 Officers disclosing information must also ensure that any information supplied is:

- necessary for the purpose for which they are sharing it;
- accurate and up-to-date;
- depersonalised (where appropriate);
- shared only with those people who need to see it; and
- transferred securely

9.4 The signatories to this protocol agree to disclose specified information to those parties identified as 'responsible authorities' or who are acting on their behalf for the purposes of sections 5 – 7 of the Crime and Disorder Act 1998 (subject to legislative amendment), namely to:

- Formulate and implement a plan for the prevention and reduction of crime and disorder in the area for each relevant period
- Carry out a review of crime patterns and levels and produce annual strategic assessments
- Produce reports to be made publicly available

9.5 When the Metropolitan Police disclose any information under this protocol, it must be in line with the Government Protective Marking System (GPMS) and marked as RESTRICTED

9.6 The disclosing officer must complete the appropriate section of the 'Request/Disclosure' Form and save it in line with service procedures.

10Security and retention

10.1 Data Protection Act

10.1.1 Partner Organisations agree to comply at all times with data protection legislation and other legal requirements relating to confidentiality.

10.2 Fair Processing

10.2.1 The Data Protection Act 1998 requires that when personal information is collected from a data subject, they are told what it will be used for and who the information will be shared with. When collecting information from clients, staff in partner organisations should explain:

- What is done with the information;
- The reason why professionals are capturing it; *and*
- Who the information can be routinely shared wit

10.2.2 Partner Organisations will ensure that their 'Fair Processing Notices' are kept up-to-date and provide an accurate explanation of the information sharing activities that are being undertaken.

10.3 Retention Periods

10.3.1 All partner organisations that are party to this protocol will put in place policies and procedures governing the retention and destruction of records containing personal information retained within their systems.

10.3.2 As a general rule, partner organisations agree that personal information that has been shared will be destroyed once it no longer is of relevance to the initial inquiry.

10.4 Data Quality

10.4.1 Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner. The data owner will be responsible for correcting the data and notifying all other recipients in writing, quoting the reference from and date of the original 'Request/Disclosure Form'.

10.5 Security

10.5.1 Personal information will be kept securely within a computer system or otherwise physically secure with appropriate levels of staff access in line with party organisations' information security policies and procedures. These policies and procedures should be based on national standards and guidance

10.5.2 Staff in Partner Organisations involved in information sharing under this protocol must:

- Be fully aware of their responsibilities under the protocol mentioned above, together with the Data Protection Act and Duty of Confidentiality.
- Use information only for the purpose stated in the original request for information.
- First obtain consent from the disclosing organisation, if they wish to pass the information onto a third party. (In a high risk situation involving safeguarding, this may not always be a reasonable requirement. In emergencies, the public interest disclosure is a sufficient exemption to override this requirement).
- Store hard copies of the request/disclosure and consent forms in a lockable container when not in use, and a clear desk policy implemented.
- If the information is held electronically, access must be restricted only to persons with a genuine 'need to know' the information.
- Once this information is no longer required, it MUST be returned to the requesting officer for destruction. Only the minimum amount of personal information should be retained which is necessary to achieve the specific objective under the Crime and Disorder Act 1998 / Housing Acts 1985/1996 or Homelessness Act 2002.

10.5.3 Each Partner Organisation is responsible for ensuring that the appropriate staff members are adequately trained in respect of all matters covered by this protocol. All temporary and agency staff will be appropriately briefed on their responsibilities as part of their induction.

10.6 Subject Access Requests

10.6.1 The Data Protection Act gives people the right to apply to an organisation that holds personal information about them for access to that information. The exercise of this right is referred to as a subject access request. People may exercise this right on their own behalf or through a representative. Where people do not have the mental capacity to make a request on their own behalf, because they are too young or for some other reason, their parent or person with Power of

Attorney may make the request on their behalf. All partner organisations that are party to this protocol will put in place procedures for handling requests for personal information.

10.6.2 The right of subject access applies to all personal information held by an organisation about that data subject regardless of whether or not that organisation is the “owner” or “source” of the information. The information must be disclosed to the data subject unless one of the exemptions in the Data Protection Act applies. It may be appropriate for the organisation that has received the subject access request to consult with the source of the information they hold to discuss whether the information is subject to an exemption.

11 Freedom of Information

11.1 The Freedom of Information Act 2000 (FOI) enables any member of the public to apply for access to information held by bodies across the public sector. The Act provides a general right of access to information held by public authorities in the course of carrying out their public functions, subject to some exemptions. This right does not extend to personal information, which is largely exempt from the Freedom of Information Act.

12 List of Appendices

A. Principal parties to the protocol
B. Information Exchange Forms for Request/Disclosure and Consent
C. Types of depersonalised data – examples
D. Simple Guide to information sharing
E. Caldicott principles
F. Statutory/legal powers to share
G. Information sharing relating to children and parental consent
H. H M Government guidance on information sharing for practitioners **(appended as a separate document)**

Appendix A – Parties to the Protocol

PRINCIPAL SIGNATORIES

Chief Executive, London Borough of Haringey

Borough Commander, Haringey Borough, Metropolitan Police Service

Borough Fire Commander, Haringey Borough, London Fire Brigade

Chief Executive, Haringey Clinical Commissioning Group

Chief Probation Officer, National Probation Service

Assistant Chief Officer, London Community Rehabilitation Company

Chief Executive, Barnet, Enfield and Haringey Mental Health Trust

Managing Director, Homes for Haringey

Director, Bridge Renewal Trust

Appendix B - Information Exchange Forms (storage and security is in here!)

Crime and Disorder Information Sharing Protocol

The following information has been supplied in accordance with Haringey's Crime and Disorder Information Sharing Protocol.

The following provisions MUST be applied in accordance to the Protocol above:

- You should be fully aware of your responsibilities under the Protocol mentioned above, together with the Data Protection Act and Duty of Confidentiality (check fully explained)

- Information shared under the terms of this protocol must only be used for the purpose stated in the original request for information.

- Information cannot be passed to a third party for any purpose other than those mentioned in section 29(1) of the Data Protection Act 1998 (DPA), without obtaining consent from the disclosing organisation. If you do wish to pass the information onto a third party, you **MUST** first obtain consent from the disclosing organisation via the designated liaison officer.

- These forms **MUST** be stored in a lockable container when not in use, and a clear desk policy implemented.

- If the information is held electronically, these forms **MUST** be placed within a folder with a secure password and access restricted only to persons with a genuine 'need to know' the information.

- Once this information is no longer required, it **MUST** be returned to the Designated Liaison Officer (DLO) for destruction.

Crime and Disorder Information Sharing Protocol
Request/Disclosure Form

PART A – INFORMATION REQUESTED - (to be completed by requesting officer)

Information requested by:

Name:	
Position:	
Organisation/Department:	
Address:	
Contact phone number:	
Email address:	

Information requested:

Describe the information required and the circumstance that have led to this request being made, including any names, addresses and dates of birth and state whether they are a victim, informant, witness suspect or convicted offender.			
Name:			
Address:			
DOB(ddmmyyyy):			

Date information is required by (ddmmyyyy):			
If urgent, please state reason:			

If a VIW or CO[1], has consent been obtained and included at Part B of this form?	
If not a VIW or CO, or no consent has been obtained, is it in the public interest to disclose?	
Please state reason for public interest:	

Under which piece of legislation: (please tick)

Crime and Disorder Act	S115- Crime Reduction Strategy	☐	S17 – Crime Reduction	☐
	S1 – ASB	☐	S2 – Sex Offender Orders	☐
	S8 – Parenting Order	☐	S11 – Child Safety Order	☐
	S15 – Local Curfew Orders	☐	Ss28-33 – Racially	☐

[1] Victim, Informant, Witness or Convicted Offender

			Aggravated Crimes	
Housing Act	S84 – application for possession order			☐
Homelessness Act	S10 – application for re-housing			☐
Anti-social Behaviour Crime & Policing Act				☐
Other (please state)				☐

Signature of requesting officer:		Date:			

PART B - INFORMATION DISCLOSED – (to be completed by disclosing officer)

Date request received:	
Disclosure Agreed:	Yes ☐ No ☐
Reason for declining request (if applicable):	
Information attached to this form	Yes ☐ No ☐

Information disclosed (Continue on a separate sheet if necessary, and remember to attach any additional sheets to this form)	

Information disclosed by:

Name:	
Position:	
Organisation:	
Department::	
Address:	
Contact phone number:	
Email address:	

Information disclosed to:

Name:	
Organisation/Department::	
Contact phone number:	

Delivery method (please mark as appropriate): Post ☐ Email ☐ Fax ☐ Other

Signature of disclosing officer: _____ Date supplied: _____

Crime and Disorder Information Sharing Protocol- Consent Form

Requesting Officer's Ref:	
Disclosing Officer's Ref:	

Please provide the relevant information below:

Is this information about you? Yes ☐ No ☐ If 'No', who is the information about? Name: Address: DOB (ddmmyyyy)   Are you are acting as: Parent/Guardian/Carer Other (please describe)

Have the reasons for requesting consent been explained to you? Yes ☐ No ☐

I give:	
consent to disclose to:	

Information to which this consent applies:

Personal information and any relevant information, for the purposes of:

Your Name:				
Address:				
DOB (ddmmyyyy):				

Signature:				
Date				

(ddmmyyyy):				

Witnessed by requesting officer:

Name:				
Position:				
Signature:				
Date (ddmmyyyy):				

Appendix C - Depersonalised Information - Examples

Police:

- MPS crime statistics;
- Local crime information (CRIS data);
- Calls for police assistance (CAD data).

Local Authorities (and registered social landlords as appropriate):

- Criminal damage and graffiti removal;
- Derelict and empty property;
- Emergency out of hours calls;
- Nuisance families and resident complaints;
- Racial, homophobic and domestic violence incidents and other forms of hate crimes;
- Re-housed homeless, victims, offenders;
- Turnover of tenants;
- Vandalism to estate lighting;
- All night cafes;
- Alcohol and entertainment licences;
- Noise levels and nuisance neighbours;
- Elderly resident locations;
- Families on benefit;
- Vulnerable persons;
- Children involved in crime;
- People undertaking drug and substance misuse treatment;
- Population data and property values;
- Leisure, youth and playground facilities;
- School exclusions.

Health:

- Accident and Emergency admissions;
- Registered alcoholics and drug users;
- Vulnerable persons;
- Ambulance control and dispatch calls;
- Mentally ill or disordered people;
- A&E hospital referrals to agreed support schemes
- Substance misuse

Probation:

- Offender profiles
- Children at risk

London Fire Brigade:

- Fires;
- Any duty under the Fire and Rescue Services Act 2004.

Appendix D: Simple Guide to information sharing and flowchat

Information sharing with consent

If you have the person's consent, then it is ok to share personal information about them. Obtaining explicit consent for information sharing is best practice in most situations but it is not always possible or appropriate to do so.

Information sharing protocols

An Information Sharing Protocol (ISP) is a signed agreement between two or more organisations relating to a specified information sharing activity. An ISP explains the terms under which the organisations have agreed to share information and the practical steps that need to be taken to ensure compliance with those terms. If there is an ISP applicable to your information sharing situation, you must follow that. ISPs are not required for information sharing. The absence of an ISP should not prevent sharing information.

The Golden Rules[2] for information sharing

Where you are considering sharing information and you do not have the person's consent and there is not an information sharing protocol in place to govern that exchange of information; following the golden rules should ensure that you strike the correct balance between protecting people's privacy and ensuring that fellow practitioners have the information they need to deliver services.

1. Remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately.

2. Be open and honest with the person 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. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

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 judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

---

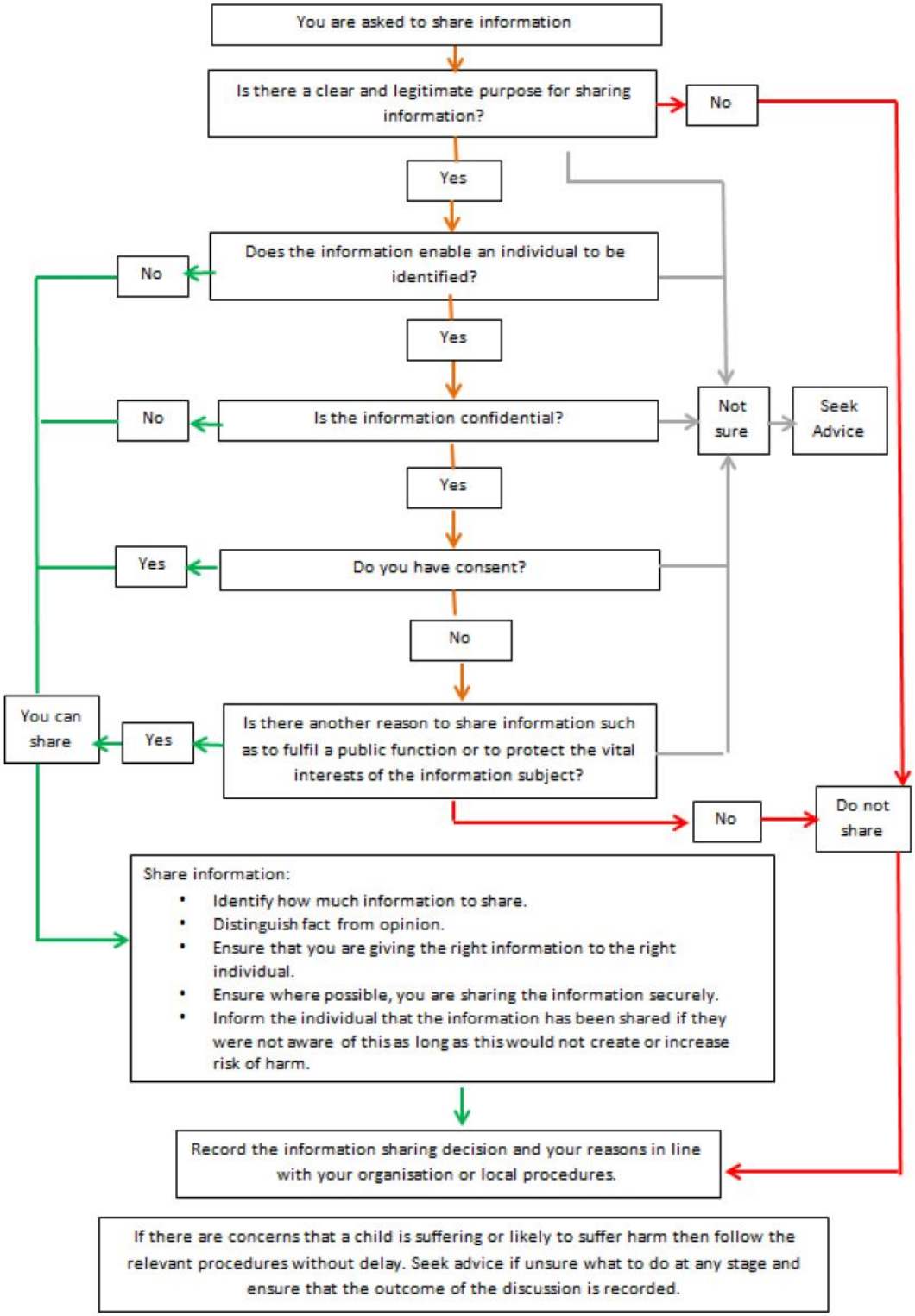
[2] The Golden Rules have been copied from "Information Sharing: Guidance for practitioners and managers" published by the Department for Children, Schools and Families, and Communities and Local Government.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for 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.

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.

Flowchart of when and how to share information



Appendix E- Caldicott principles

1. Justify the purpose(s)
Every proposed use or transfer of identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use identifiable information unless it is necessary
Identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for subjects to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary identifiable information
Where use of identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. Access to identifiable information should be on a strict need-to-know basis
Only those individuals who need access to identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. Everyone with access to identifiable information should be aware of their responsibilities
Action should be taken to ensure that those handling identifiable information are made fully aware of their responsibilities and obligations to respect confidentiality.

6. Understand and comply with the law
Every use of identifiable information must be lawful. Someone in each organisation handling information should be responsible for ensuring that the organisation complies with legal requirements.

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

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

APPENDIX F

LEGAL POWERS TO SHARE INFORMATION

The Children Act 1989

Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Section 47 states that unless in all the circumstances it would be unreasonable for them to do so, the following authorities must assist a local authority with these enquiries if requested, in particular by providing relevant information:

- any local authority;
- any local education authority;
- any housing authority;
- any health authority;
- any person authorised by the Secretary of State.

A local authority may also request help from those listed above in connection with its functions under Part 3 of the Act. Part 3 of the Act, which comprises of sections 17-30, allows for local authorities to provide various types of support for children and families. In particular, section 17 places a general duty on local authorities to provide services for children in need in their area. Section 27 enables the authority to request the help of one of those listed above where it appears that such an authority could, by taking any specified action, help in the exercise of any of their functions under Part 3 of the Act. Authorities are required to co-operate with a request for help so far as it is compatible with their own statutory duties and does not unduly prejudice the discharge of any of their functions.

The Children Act 2004

Section 10 of the Act places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to:

- Physical and mental health, and emotional well-being;
- Protection from harm and neglect;
- Education, training and recreation;
- Making a positive contribution to society;
- Social and economic well-being.

The relevant partners must co-operate with the local authority to make arrangements to improve the well- being of children. The relevant partners are:

- district councils;
- the police;
- the Probation Service;
- youth offending teams (YOTs);

- strategic health authorities and primary care trusts;
- Connexions;
- the Learning and Skills Council.

This statutory guidance for section 10 of the Act states good information sharing is key to successful collaborative working and arrangements under this section should ensure information is shared for strategic planning purposes and to support effective service delivery. It also states these arrangements should cover issues such as improving the understanding of the legal framework and developing better information sharing practice between and within organisations.

Section 11 of the Act places a duty on key persons and bodies to make arrangements to ensure their functions are discharged with regard to the need to safeguard and promote the welfare of children. The key people and bodies are:

- local authorities (including district councils);
- the police;
- the Probation Service;
- bodies within the National Health Service (NHS);
- Connexions;
- YOTs;
- governors/directors of prisons and young offender institutions;
- directors of secure training centres;
- the British Transport Police.

The section 11 duty does not give agencies any new functions, nor does it override their existing ones, it simply requires them to:

- carry out their existing functions in a way that takes into account the need to safeguard and promote the welfare of children;
- ensure services they contract out to others are provided having regard to this need (to safeguard and promote the welfare of children).

In order to safeguard and promote the welfare of children, arrangements should ensure that:

- all staff in contact with children understand what to do and are aware of the most effective ways of sharing information if they believe a child and family may require targeted or specialist services in order to achieve their optimal outcomes;
- all staff in contact with children understand what to do and when to share information if they believe that a child may be in need, including those children suffering or at risk of significant harm.

Education Act 2002

The duty laid out in section 11 of the Children Act 2004 mirrors the duty imposed by section 175 of the Education Act 2002 on LEAs and the governing bodies of both maintained schools and further education institutions. This duty is to make arrangements to carry out their functions with a view to safeguarding and promoting the welfare of children and follow the guidance in *Safeguarding Children in Education* (DfES 2004).

The guidance applies to proprietors of independent schools by virtue of section 157 of the Education Act 2002 and the Education (Independent Schools Standards) Regulations 2003.

Section 21 of the Act, as amended by section 38 of the Education and Inspections Act 2006, places a duty on the governing body of a maintained school to promote the well-being of pupils at the school. Well-being in this section is defined with reference to section 10 of the Children Act 2004 (see paragraph 5.5 above). The Act adds that this duty has to be considered with regard to any relevant children and young person's plan.

This duty extends the responsibility of the governing body and maintained schools beyond that of educational achievement and highlights the role of a school in all aspects of the child's life. Involvement of other services may be required in order to fulfil this duty so there may be an implied power to work collaboratively and share information for this purpose.

Education Act 1996

Section 13 of the Education Act 1996 provides that an LEA shall (so far as their powers enable them to do so) contribute towards the spiritual, moral, mental and physical development of the community, by securing that efficient primary and secondary education is available to meet the needs of the population of the area. Details of the number of children in the local authority's area and an analysis of their needs are required in order to fulfil this duty, therefore there may be an implied power to collect and use information for this purpose.

Section 408 and the Education (Pupil Information)(England) Regulations 2005 requires the transfer of the pupil's common transfer file and educational record when a pupil changes school.

Section 434 (4) of the Act requires LEAs to request schools to provide details of children registered at a school.

Learning and Skills Act 2000

Section 117 of the Learning and Skills Act 2000 provides for help to a young person to enable them to take part in further education and training.

Section 119 enables Connexions Services to share information with Jobcentre Plus to support young people to obtain appropriate benefits under the Social Security Contributions and Benefits Act 1992 and Social Security Administration Act 1992.

Education (SEN) Regulations 2001

Regulation 6 provides that when the LEA is considering making an assessment of a child's special educational needs, it is obliged to send copies of the notice to social services, health authorities and the head teacher of the school (if any) asking for relevant information.

Regulation 18 provides that all schools must provide Connexions Services with information regarding all Year 10 children who have a statement of special educational needs.

Children (Leaving Care) Act 2000

The main purpose of the Act is to help young people who have been looked after by a local authority, move from care into living independently in as stable a fashion as possible. To do this it amends the Children Act 1989 (c.41) to place a duty on local authorities to assess and meet need. The responsible local authority is under a duty to assess and meet the care and support needs of **eligible** and **relevant** children and young people and to assist **former relevant children**, in particular in respect of their employment, education and training.

Sharing information with other agencies will enable the local authority to fulfil the statutory duty to provide after care services to young people leaving public care.

Mental Capacity Act 2005

The Mental Capacity Act 2005 (MCA) and the associated Code of Practice contain guidance that is applicable to considerations of a person's capacity or lack of capacity to give consent to information sharing.

Section 1 of the MCA sets out 5 statutory principles on capacity:

- A person must be assumed to have capacity unless it is established that they lack capacity.

- A person is not to be treated as unable to make a decision unless all practicable steps to help him to do so have been taken without success.

- A person is not to be treated as unable to make a decision merely because he makes an unwise decision.

- An act carried out or a decision made, under this Act for or on behalf of a person who lacks capacity, must be done in his best interests.

- Before the act is done, or the decision is made, regard must be had to whether the purpose for which it is needed can be as effectively achieved in a way that is less restrictive on the person's rights and freedom of action.

Mental Capacity Act 2005 Code of Practice

Chapter 4 of the Mental Capacity Act 2005 Code of Practice provides guidance on how to assess whether someone has the capacity to make a decision. In this chapter, as throughout the Code, a person's capacity (or lack of capacity) refers specifically to their capacity to make a particular decision at the time it needs to be made.

Assessing capacity: Anyone assessing someone's capacity to make a decision for themselves should use the two-stage test of capacity:

- Does the person have an impairment of the mind or brain, or is there some sort of disturbance affecting the way their mind or brain works? (It doesn't matter whether the impairment or disturbance is temporary or permanent).
- If so, does that impairment or disturbance mean that the person is unable to make the decision in question at the time it needs to be made?

Assessing ability to make a decision

- Does the person have a general understanding of what decision they need to make and why they need to make it?
- Does the person have a general understanding of the likely consequences of making, or not making, this decision?
- Is the person able to understand, retain, use and weigh up the information relevant to this decision?
- Can the person communicate their decision (by talking, using sign language or any other means)? Would the services of a professional (such as a speech and language therapist) be helpful?

Assessing capacity to make more complex or serious decisions

- Is there a need for a more thorough assessment (perhaps by involving a doctor or other professional expert)?

Immigration and Asylum Act 1999

Section 20 provides for a range of information sharing for the purposes of the Secretary of State:

- to undertake the administration of immigration controls to detect or prevent criminal offences under the Immigration Act;
- to undertake the provision of support for asylum seekers and their dependents.

Criminal Justice Act 2003

Section 325 of this Act details the arrangements for assessing risk posed by different offenders:

- The "responsible authority" in relation to any area, means the chief officer of police, the local probation board and the Minister of the Crown exercising functions in relation to prisons, acting jointly.

- The responsible authority must establish arrangements for the purpose of assessing and managing the risks posed in that area by:

    a) relevant sexual and violent offenders; and
    b) other persons who, by reason of offences committed by them are considered by the responsible authority to be persons who may cause serious harm to the public (this includes children)

- In establishing those arrangements, the responsible authority must act in co-operation with the persons identified below

- Co-operation may include the exchange of information.

The following agencies have a duty to co-operate with these arrangements:

a) every youth offending team established for an area
b) the Ministers of the Crown, exercising functions in relation to social security, child support, war pensions, employment and training
c) every local education authority
d) every local housing authority or social services authority
e) every registered social landlord who provides or manages residential accommodation
f) every health authority or strategic health authority
g) every primary care trust or local health board
h) every NHS trust
i) every person who is designated by the Secretary of State as a provider of electronic monitoring services

National Health Service Act 1977

The National Health Service Act 1977 Act provides for a comprehensive health service for England and Wales to improve the physical and mental health of the population and to prevent, diagnose and treat illness.

Section 2 of the Act provides for sharing information with other NHS professionals and practitioners from other agencies carrying out health service functions that would otherwise be carried out by the NHS.

National Health Service Act 2006

Section 82 of the National Health Service Act 2006 places a duty on NHS bodies and local authorities to co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.

The Adoption and Children Act 2002

The Adoption and Children Act 2002 and the associated Regulations make provision for obtaining, recording and keeping confidential information about adopted children and/or their relatives. The Act and Regulations, give limited express power to share information, in prescribed circumstances as laid out in the legislation. Information about pre-2002 Act adoptions remains governed by the provisions of the Adoption Agencies Regulations 1983. Legal advice should be sought before any disclosure from adoption records.

The Care and Support Statutory Guidance issued under the Care Act 2014

The guidance under the heading "Reporting and responding to abuse and neglect" provides that

"14.34. Early sharing of information is the key to providing an effective response where there are emerging concerns (see information sharing (14.150) and confidentiality (14.157) section). To ensure effective safeguarding arrangements:

- all organisations must have arrangements in place which set out clearly the processes and the principles for sharing information between each other, with other professionals and the SAB (Safeguarding Adult Board); this could be via an Information Sharing Agreement to formalise the arrangements; and,

- no professional should assume that someone else will pass on information which they think may be critical to the safety and wellbeing of the adult. If a professional has concerns about the adult's welfare and believes they are suffering or likely to suffer abuse or neglect, then they should share the information with the local authority and, or, the police if they believe or suspect that a crime has been committed."

The Working Together to Safeguard Children Guidance 2015

The guidance provides that

> "22. Effective sharing of information between professionals and local agencies is essential for effective identification, assessment and service provision.
>
> 23. Early sharing of information is the key to providing effective early help where there are emerging problems. At the other end of the continuum, sharing information can be essential to put in place effective child protection services. Serious Case Reviews (SCRs) have shown how poor information sharing has contributed to the deaths or serious injuries of children.
>
> 24. 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. To ensure effective safeguarding arrangements:
>
> - all organisations should have arrangements in place which set out clearly the processes and the principles for sharing information between each other, with other professionals and with the LSCB; and
> - no professional should assume that someone else will pass on information which they think may be critical to keeping a child safe. If a professional has concerns about a child's welfare and believes they are suffering or likely to suffer harm, then they should share the information with local authority children's social care.
>
> 25. *Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (2015)* supports frontline practitioners, working in child or adult services, who have to make decisions about sharing personal information on a case by case basis.6 The advice includes the seven golden rules for sharing information effectively and can be used to supplement local guidance and encourage good practice in information sharing.

APPENDIX G

Request for information relating to children and parental consent

1 Partner Organisations must have regard to the Working Together to Safeguard Children 2015 Guidance; Information sharing: advice for practitioners providing safeguarding services to children, young people, parents and carers (2015); and The London Child Protection Procedures 2015 when considering referrals that require the sharing of information.

2. Partner Organisations must consider whether to seek consent from the child or young person of sufficient age and understanding or their parents where appropriate, to share their personal information with other partner agencies. Obtaining informed and explicit consent for information sharing is very important and ideally should be obtained from the start.

3. Partner Organisations should be open and honest with the person (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.

4. There are a range of circumstances where the obligation to seek consent (from a child or young person of sufficient age and understanding or a parent) does not apply. These include circumstances where seeking consent would:

   a) place a person (the individual, family member, yourself or a third party) at increased risk of significant harm if a child, or serious harm if an adult; or

   b) prejudice the prevention, detection or prosecution of a serious crime; or

   c) lead to an unjustified delay in making enquiries about allegations of significant harm to a child, or serious harm to an adult.

   These circumstances are not confined to cases where the Section 47 threshold has been met. If at the relevant time the Section 47 threshold is not met and one of the other circumstances in 4 (a) to (c) above is met, the decision can be made not to seek consent.

5. Where possible, the wishes of children, young people or parents who do not consent to share confidential information should be respected. However, information may still be shared without consent if, in the partner

agency judgement based on the facts of the case there is sufficient need in the public interest to override an absence of consent to protect the welfare of a child.

6. Partner Organisations must ensure that information shared is necessary, proportionate, relevant, accurate, timely and secure. The information share must be necessary for the purpose for which it is shared; it is shared only with agencies that need to have it; it is accurate and up-to-date; it is shared in a timely fashion, and is shared securely.

7. Where consent is refused to share information, this may be additional information on which to make a judgement on whether the child is at risk of significant harm or there is a need to investigate the issue further. The recording of the decision to proceed without parental consent in either of these scenarios or for other reasons is therefore essential.

8. Where consent is sought, it must be properly informed, which means that the person giving consent needs to understand why information needs to be shared, what will be shared, who will see their information, the purpose for which it will be put and the implications of sharing that information. They will need to be told, in general terms, what questions the Partner Organisation wishes to ask, of whom, why, and what information the Organisation will be providing to external persons or bodies in the course of making its enquiries.

9 Partner Organisation must keep record of all information sharing decision. The record should include:

a) the date and time;
b) a summary of the information;
c) the requestor's name, job title, organisation;
d) partner agency decision (whether to share or not) and the reasons for this decision;
e) whether you are sharing with or without consent;
f) if sharing without consent, whether the person or family were informed and, if not why not;
g) who consented or authorised the information sharing, if appropriate;
h) what type of information was shared (but not the content); and
i) how the information was shared (email, phone etc);