

# INFORMATION SHARING PROTOCOL

for ALL AGENCIES & PRACTITIONERS WORKING WITH CHILDREN  
& YOUNG PEOPLE



Document Title	Version & Date Approved	Date Published	Next Review Due Date
SCSP Information Sharing Multi-Agency Protocol	V1 – May 2022	June 2022	November 2023

## CONTENTS

1. INTRODUCTION.....	3
2. PURPOSE OF THIS PROTOCOL.....	4
3. WHAT IS INFORMATION SHARING.....	5
4. LEGAL BASIS FOR INFORMATION SHARING.....	6
5. THE PRINCIPLES OF INFORMATION SHARING.....	7
6. INFORMATION SHARING & CONSENT IN SAFEGUARDING.....	9
7. CALDICOTT PRINCIPLES.....	10
8. SHARING INFORMATION APPROPRIATELY AND SECURELY.....	10
9. METHODS OF REQUESTING AND TRANSFERRING INFORMATION.....	10
10. STORAGE OF INFORMATION.....	11
11. INDIVIDUAL RIGHTS.....	11
12. FREEDOM OF INFORMATION REQUESTS.....	11
13. COMPLAINTS AND BREACHES.....	11
14. DISAGREEMENT AROUND INFORMATION SHARING.....	12
15. APPENDIX 1.....	13
16. INFORMATION SHARING RESPONSIBILITIES.....	13
17. APPENDIX 2.....	15
18. GUIDANCE TO ASSIST WITH THE DECISION MAKING IN RELATION TO SHARING INFORMATION.....	15
19. APPENDIX 3.....	20
20. SEVEN GOLDEN RULES FOR INFORMATION SHARING.....	20
21. APPENDIX 4.....	21
22. FLOWCHART OF WHEN AND HOW TO SHARE INFORMATION.....	21
23. APPENDIX 5.....	22
24. SIGNATORIES TO THIS PROTOCOL.....	22

## 1 Introduction

1.1 This document has been developed to address information sharing both at strategic and operational levels for all who are involved within the arenas of Safeguarding Children, young people and families across Sandwell. It is the overarching information sharing protocol and is designed to support effective communication between professionals and will ensure better understanding of what information should be shared, with whom and under what circumstances, and the dangers of not doing so.

1.2 In line with Working Together we know that:

“Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe. Serious case reviews (SCRs<sup>1</sup>) have highlighted that missed opportunities to record, understand the significance of and share information in a timely manner can have severe consequences for the safety and welfare of children”.

1.3 Information sharing is a vital part of ensuring that professionals can effectively assess the needs of a child or the risks to a child. Often it is only when information from all sources has been shared that it becomes clear that a child has suffered, or is likely to suffer, significant harm. Early sharing of information is also the key to providing effective Early Help where there are emerging problems. Local Children Safeguarding Practice Reviews (LCSPRs) have shown how poor information sharing has contributed to the deaths or serious injuries of children and Working Together 2018<sup>2</sup> is absolutely clear that *“Effective sharing of information between practitioners and local organisations and agencies is essential for early identification of need, assessment and service provision to keep children safe.”* Working Together to Safeguard Children 2018 requires the Statutory Safeguarding Partners to set out how they will work together and with any relevant agencies to ensure that children are safeguarded, and their welfare promoted. Partners who are listed as relevant agencies within the SCSP MASA 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. This Protocol has been produced by the SCSP to ensure there is a uniformed approach to information sharing by all safeguarding partners in Sandwell.

---

<sup>1</sup> <https://www.gov.uk/government/publications/analysis-of-serious-case-reviews-2011-to-2014>

## Who should use this Protocol?

- 1.4 This Protocol is applicable to all those working with children and young people as an employee of any of the Statutory Safeguarding Partners of Sandwell Children's Safeguarding partnership (SCSP), this includes;
- Sandwell Metropolitan Borough Council (SMBC)
  - Sandwell Children's Trust (SCT)
  - Black Country and West Birmingham Clinical Commissioning Group (BCCCG).
  - West Midlands Police (WMP).
- In addition, the guidance is applicable to all schools /colleges and relevant agencies with safeguarding responsibilities and listed under Section 11 of the Children Act 2004

## The purpose of this Protocol is to:

Outline the principles and practice which govern the sharing of information between agencies, for the purposes of safeguarding and promoting the welfare and protection of children and young people, whilst ensuring that legislation and government guidelines are followed for effective and lawful sharing of information by all practitioners.

- 1.5 Appendices have been included to provide additional guidance to assist professionals with decision making around information sharing.
- 1.6 This Protocol complies with the UK General Data Protection Regulations (UK GDPR) and Data Protection Act 2018.
- 1.7 This protocol also takes account of the guidance from the Information Commissioner's Office [ICO]. The SCSP recommends that 'legal obligation' and 'public task' (as defined in the UK GDPR) are relied on as the primary basis for processing information to establish whether or not there is a need to safeguard the welfare of a child. This means that, whilst families will be informed when personal data is being shared or processed, their consent is not required. The significance of this is that it is not necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of a child (i.e. removing the distinction between information sharing for the purposes of assessing need or child protection). The preference should always be to inform parents / carers that information will be shared for these purposes and to seek to work cooperatively with them and to also ensure that parents / carers are aware that information is shared, processed and stored for these purposes.

Working Together 2018 Guidance also emphasises the use of consent. The SCSP is working to ensure that the approach taken in this Protocol is consistent with the Data

Protection Act 2018, the guidance published by the ICO and the statutory guidance published by the Department for Education. References to consent and information sharing in this Protocol will be highlighted with a link to the relevant national guidance.

### **This Protocol should be read in conjunction with:**

- The Information Commissioner's Office Data Sharing Code of Practice: This is a statutory code which explains how the Data Protection Act applies to the sharing of personal data. It provides practical advice to all organisations, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one-off requests to share personal data.
- The Government's Information Sharing Advice for safeguarding practitioners: This advice is for front-line practitioners and senior managers. It helps them decide when and how to share personal information legally and professionally.
- The West Midlands Regional Safeguarding Procedures: <https://westmidlands.procedures.org.uk/pkphs/regional-safeguarding-guidance/information-sharing-and-confidentiality>

### **WHAT IS INFORMATION SHARING?**

1.8 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** – 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.
- **Sharing** - in which agencies pool available data and maintain single service-based records.
- **Exchange** – in which one agency provides one or more other agencies with relevant data. Ownership and responsibility pass to the new agency which may amend or update the record to meet further requirements.
- **Reporting** - an agency provides statistical data for an agreed reporting mechanism which may be reported to local and national groups.

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

- **Organisational material** - plans, policies, guidelines, minutes of meetings. 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, the SCSP is currently exempt from the FOI legislation and is 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.

- **Statistical material** – aggregated or anonymised data including relevant analysis. 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.
- **Personal data** - (as defined by the Data Protection Act 2018) is:
  - 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.

## LEGAL BASIS FOR INFORMATION SHARING

1.10 When deciding whether to share personal data for the purpose of safeguarding children, practitioners must first establish whether there is a legal basis to share the information. In addition to the statutory guidance following from the Children Act 2004<sup>3</sup>, the four main areas of law, key concepts, and terminology that relate to the disclosure and sharing of information are:

- The Data Protection Act 2018<sup>4</sup>
- General Data Protection Regulations 2018/UK GDPR<sup>5</sup>.
- The Human Rights Act 1998<sup>6</sup>
- The Common Law Duty of Confidentiality<sup>7</sup>

1.11 Article 8 of the European Convention on Human Rights gives everyone a right to have 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.

---

<sup>3</sup> <https://www.legislation.gov.uk/ukpga/2004/31/contents>

<sup>4</sup> <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

<sup>5</sup> <https://www.gov.uk/government/publications/data-protection-law-eu-exit>

<sup>6</sup> <https://www.legislation.gov.uk/ukpga/1998/42/contents>

<sup>7</sup> <https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality>

- 1.12 The implementation of the Data Protection Act 2018 and GDPR (now UK GDPR) broadened the scope of the legislation to incorporate the processing of personal data for safeguarding purposes within organisations. This is 'special category data' which relates to personal information of subjects which is especially sensitive and personal, the exposure of which could significantly impact the rights and freedoms of data subjects.
- 1.13 Where practitioners need to share special category personal data they should be aware that the Data Protection Act 2018 includes the 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent and can be used for the purposes of:
- protecting an individual from neglect or physical, mental or emotional harm or
  - protecting the physical, mental or emotional wellbeing of an individual.
- 1.14 This therefore applies to safeguarding children and the legislation broadens the scope of what is meant by 'special category data'.
- 1.15 All information shared between agencies must have a defined and justifiable purpose and the information shared must be accurate and necessary for the purpose for which it is being shared; the information must be shared securely and shared only with those who need to see it.
- 1.16 Safeguarding and promoting the safety and welfare of children is the prime consideration in all decision making about sharing information.
- 1.17 The legal basis supports the functions of the SCSP for quality assurance of multi-agency practice involving joint audits of case files and case reviews involving practitioners for the purpose of identifying lessons learned. This makes allowances for 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.
- 1.18 In addition, 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 (including organisations providing statutory children social care services), Health Authorities (CCG) and the Probation Service.

## **THE PRINCIPLES OF INFORMATION SHARING**

- 5.1 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 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.

5.2 The principles set out below are intended to help practitioners working with children, young people, 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 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.

5.3 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 including others who may be at risk.

5.4 Remember that using **professional curiosity** can help to prevent risk. If there are concerns that a child 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.



5.5 See the following additional guidance & resources:

- Appendix 1:** Information Sharing Responsibilities for the SCSP Partners,  
**Appendix 2:** Guidance to assist with decision making in relation to sharing information,  
**Appendix 3:** Seven Golden Rules of Information Sharing.  
**Appendix 4:** Information Sharing Flowchart.

## **INFORMATION SHARING & CONSENT IN SAFEGUARDING**

- 6.1 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 condition that allows practitioners to share information without consent.
- 6.2 Practitioners should proactively inform children, parents and carers when they first engage with the service about the organisation's policy on how information is shared and the basis (Data Protection Act 2018/UK GDPR) upon which their personal data is being processed.
- 6.3 Information may be shared without consent if a practitioner has reason to believe that there are grounds to do so and that the sharing of the information will enhance the safeguarding of the child in a timely manner.

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

- place a child (the individual, family member, staff or a third party) at increased risk of significant harm, or
  - prejudice the prevention, detection or prosecution of a serious crime and/or lead to an unjustified delay in making enquiries about allegations of significant harm to a child
  - 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. 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 GDPR expressly states that where there is an imbalance of power in a business context/relationship, consent will not be a valid condition for using data.
- 6.4 When deciding whether to share confidential information the practitioner must judge on the facts of the case whether the sharing of the information is a necessary and proportionate response to the need to protect the child, or the wider public from serious harm.
- 6.5 Sharing confidential information without consent will normally be justified in the public or vital interest when:

- there is evidence or reasonable cause to believe a child is suffering or is at risk of suffering significant harm,
- to prevent significant harm to a child including the wider public including through the prevention, detection and prosecution of a serious crime,
- where there is an imbalance of power between the parties.

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

6.7 Consent should not be sought when there is a requirement by law to share information through a statutory duty or by a court order.

## **CALDICOTT PRINCIPLES**

7.1 The Caldicott Principles and HM Government advice<sup>8</sup> for practitioners on 7 Golden Rules are helpful in considering the justification for the sharing of information.

## **SHARING INFORMATION APPROPRIATELY AND SECURELY**

8.1 Practitioners must have due regard to the relevant data protection principles which allow them to share information as outlined in the Data Protection Act 2018 and the UK GDPR. To share information effectively practitioners should:

- Be confident of the processing conditions under the Data Protection Act 2018 and UK GDPR which allow 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'.
- In respect of special category data be aware that the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information. This includes allowing practitioners to share information without consent if it is not possible to gain consent, it cannot be reasonably expected that a practitioner gains consent or gaining consent would place a child at risk.

## **METHODS OF REQUESTING AND TRANSFERRING INFORMATION**

9.1 Information will normally be exchanged electronically by secure encrypted email. The SCSP's Business Unit email is: [SCSP\\_Business@sandwell.gov.uk](mailto:SCSP_Business@sandwell.gov.uk)

---

8

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/251750/9731-2901141-TSO-Caldicott-Government\\_Response\\_ACCESSIBLE.PDF](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF)

## **STORAGE OF INFORMATION**

10.1 Each signatory to this protocol:

- will ensure storage of all paper and electronic records adheres to the requirements of the Data Protection Act 2018 and any associated local and national information governance policy.
- will ensure that all information is transmitted safely and securely in compliance with the Data Protection Act 2018.
- is responsible for protecting the personal and confidential data meeting the requirements of the Data Protection Act 2018.
- must have in place governance agreements which comply with the Data Protection Act 2018.
- must ensure all 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.

## **INDIVIDUAL RIGHTS**

11.1 Subject Access under GDPR/Data Protection Act 2018 –

- 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, the right to rectify, object or erase. An Information Rights Request to the SCSP should be forwarded to Sandwell Metropolitan Borough Council's Data Protection Team:

[CS\\_Firmstep@sandwell.gov.uk](mailto:CS_Firmstep@sandwell.gov.uk)

## **FREEDOM OF INFORMATION REQUESTS**

12.1 The SCSP is a statutory partnership established under the Social Work Act 2017 and it is not a public authority for the purposes of the Freedom of Information Act 2000. The partnership is therefore exempt from the duty to provide information though it will consider requests on an individual basis.

12.2 In all instances no records of meetings will be shared without the express permission of the Statutory Safeguarding Partners/Chair. All requests should be submitted to the SCSP Business Unit - [SCSP\\_Business@sandwell.gov.uk](mailto:SCSP_Business@sandwell.gov.uk)

## **COMPLAINTS AND BREACHES**

13.1 Breaches reported by a member of the public will usually present as a complaint. Every organisation should have their own complaints procedure, which should be adhered to should a client/service user and/or member of the public wishes to make a complaint or report an incident.

- 13.2 Each organisation should have an information governance policy which should be compliant with the Data Protection Act 2018. Any inadvertent disclosure of information by an employee must be investigated in line with internal procedures.
- 13.3 Further information on how to manage a data protection breach, including how to report a breach is available from the Information Commissioner's Office<sup>9</sup>.
- 13.4 In order to be able to monitor adherence to the Code, as effectively as possible and to consider corrective action where appropriate, it is important that information on all breaches is collated. Procedures should therefore be put in place within each organisation to ensure that details of complaints relating to the inappropriate disclosure of information (and the outcomes) are collated and reviewed on a regular basis.
- 13.5 Each agency will be held responsible for any misuse of the information supplied to it and the consequences of such misuse by its employees or agents.

## **DISAGREEMENT AROUND INFORMATION SHARING**

- 14.1 Where there is disagreement between professionals or agencies about the way information is being shared or in relation to a decision not to share information, the SCSP Resolution and Escalation Policy should be followed: <https://www.sandwellcsp.org.uk/?s=escalation>
- 14.2 Whilst this Protocol provides a framework and set of principles for sharing information in line with SCSP's MASA, to safeguard and promote the welfare of children and young people, more detailed information sharing agreements may need to be drawn up between individual agencies or groups of agencies for specific purposes. Where this is required, it should always be done with support from relevant organisational information sharing leads.
- 14.3 Alongside this Protocol, individual agencies should also refer to their own Information Governance Policy and any other organisational or sector specific guidance.
- 14.4 It is expected that agencies and professionals working with children and families in Sandwell adhere to this Protocol and supply information within the bounds of this guidance. This will help ensure the right help and support can be provided at the right time, and that the best outcomes are achieved for children and families. The members of SCSP will be asked to re-affirm their commitment to this code on a biennial basis.

---

<sup>9</sup> <https://ico.org.uk/for-organisations/report-a-breach/>

## **APPENDIX 1**

### **Information Sharing Responsibilities**

#### **Responsibilities of Sandwell Children's Safeguarding Partnership (SCSP)**

The SCSP is responsible for:

- Ensuring this Protocol is regularly reviewed and kept up to date
- Disseminating relevant learning in relation to sharing and storing information, for example learning that arises from the escalation of concerns, from Child Safeguarding Practice Case Reviews, auditing or other quality assurance activities
- Ensuring that SCSP multi-agency training supports the effective implementation of this Procedure. This includes ensuring that the key principles are embedded throughout the SCSP's training courses and is a standalone training course.
- Ensuring that relevant concerns, risks or areas of good practice in relation to sharing or storing information are discussed by the SCSP and its Sub Groups and that any appropriate action is agreed and taken forward.
- Using the SCSP Quality Assurance Framework to review whether agencies are effectively sharing and storing information. This includes using the Section 11 self-assessment criteria to evaluate whether agencies have effective mechanisms in place to ensure information is shared and stored in line with this Protocol
- Where necessary, seeking additional legal or specialist advice and guidance to support multi-agency discussion around effective information-sharing.

#### **RESPONSIBILITIES OF INDIVIDUAL AGENCIES**

All agencies (statutory and non-statutory) working with and / or providing services for children and young people in Sandwell are responsible for:

- Contributing to the development of trust and confidence between agencies by working within the framework of this Protocol
- Having effective mechanisms in place to ensure this Protocol is fully implemented, and that staff and volunteers know of its existence
- Ensuring that all staff and volunteers who are in contact with children understand what to do and the most effective ways of sharing information if they believe that a child and family may require a particular service in order to achieve positive outcomes. This includes being able to understand and apply good practice in sharing information at an early stage as part of early help or preventative work
- Ensuring that all staff and volunteers who are in contact with children understand what to do and when to share information if they believe that a child may be a child in need or a child who has suffered / is likely to suffer significant harm
- Ensuring appropriate agency or sector specific guidance is available to complement this Protocol and the legislative and government guidance
- Ensuring that an appropriate level of training on information sharing is made available to staff as part of their induction and ongoing training

- Ensuring that any problems encountered by staff in relation to the sharing or storing of information are recorded, and that this is reviewed on a regular basis to identify any concerns
- Ensuring that requirements in relation to information sharing are embedded into commissioning processes and effective monitoring of service level agreements
- Analysing any complaints relating to information sharing in order to improve practice, and where relevant sharing learning with the SCSP for wider circulation
- Ensuring that any reported breaches of the code are followed up in accordance with this Protocol and their agencies internal procedures
- Sharing improvements that have been made in relation to information sharing with the SCSP so that relevant learning can be shared across the partnership
- Supporting common systems and joint approaches that will promote effective information sharing between agencies
- Being transparent around information sharing and encouraging children and their parents to see information sharing in a positive light, as something which makes it easier for them to receive the services they need
- Ensuring that the organisation is properly registered with the Information Commissioner
- Ensuring that requests and responses to requests are sent by a secure method agreed between the services
- Ensuring that information is not kept for longer than is necessary and that there is adherence to agency or sector specific retention schedules.

Each agency should have in place a lead information officer who is responsible for decisions relating to information sharing within the agency, or between the agency and a third party and who can assist in the resolution of challenges as well as providing advice and guidance.

## **RESPONSIBILITIES OF PROFESSIONALS**

All professionals (including volunteers) working with children and young people in Sandwell are responsible for:

- Adhering to this Protocol and sharing information in line with this procedure. This includes clearly recording decisions about whether or not to share information.
- Raising with their line manager / safeguarding lead any training or learning requirements in relation to information sharing
- Recording and raising with their line manager / safeguarding lead any breaches of this Protocol or any concerns about the way information is being shared and stored either within their own agency or in other agencies.
- Ensuring that anyone who provides personal information is given details of how that information may be used, made aware of their rights in relation to information disclosure and their right of access to information they have provided, and given details of how to make a complaint.

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, they should make a referral to MASH in line with SCSP procedures.

## RESPONSIBILITIES OF AGENTS & SUB-CONTRACTORS

Each agency shall ensure that its commissioning arrangements comply with this Protocol. Commissioning and contract monitoring processes should allow commissioners to have assurance that services are being delivered in line with these procedures.

Commissioned services and professionals working within commissioned services have the same responsibilities as those of agencies and professionals set out above.

## APPENDIX 2

### Guidance to assist with decision making in relation to sharing information

Effective interagency working is dependent upon appropriate and timely information sharing whether a child or young person just needs some additional support (Early Help) or whether there are concerns that they are at risk of significant harm (safeguarding).

The Information Commissioner's Office has produced some case studies<sup>10</sup> that present a number of different scenarios relating to information sharing. These practical examples may be helpful for individual professionals when making decisions around information sharing or could be used as a resource for training or group discussion.

#### Early Help

Early Help in Sandwell includes any help or support that is provided to a child or family across levels 1-3 of our Thresholds document<sup>11</sup>. At this level, a child or family may have complex and /or multiple needs but the threshold for statutory intervention led by Sandwell Children's Trust (SCT) has not been met. This means the child is not assessed to be at risk of significant harm.

At this level of need freely given, informed explicit consent is needed. Where a professional believes they need to share information to help them understand the needs of a child / family, or to enable the child / family to receive a service from another agency, they should seek consent from all the relevant individuals before information is shared or requested. This will ensure that the child / family understand the issues and it will support good engagement by the child / family with services.

---

<sup>10</sup> <https://ico.org.uk/media/for-organisations/documents/1625861/data-sharing-code-of-practice-additional-case-studies-201701.pdf>

<sup>11</sup> <https://www.sandwellcsp.org.uk/wp-content/uploads/2021/04/SCSP-Multi-agency-Thresholds-Document-April-2021.pdf>

## **Safeguarding**

If a professional has a safeguarding concern about a child, they should discuss with their line manager or designated safeguarding lead without delay to agree the most appropriate course of action.

If there is reasonable cause to believe that the child has suffered, or is likely to suffer significant harm, then consent is not required in order to make a referral to SCT via MASH. However, in most cases it remains good practice to obtain consent (which should be freely given, informed and explicit), and professionals should still seek to discuss their concerns with the family and seek their agreement to making a referral. This will help the family to understand the concerns and why they will be contacted by SCT.

In some situations, it may be unclear whether or not the threshold for referral to MASH has been met. In these situations, the concern must not be ignored. Professionals should talk to their agency's designated safeguarding lead and, if necessary their lead officer.

For information sharing to assist with decision making. The safety and wellbeing of the child must be the overriding consideration in making any decisions whether or not to seek consent.

### **Information sharing with regards to Local Children Safeguarding Practice Reviews**

As part of the statutory function of the Safeguarding Children's Partnership there is a requirement to conduct Local Children's Safeguarding Practice Reviews (LCSPR'S) when a safeguarding concern has arisen that meets the criteria for commissioning a LCSPR.

There will be a responsibility on all agencies, statutory or otherwise, to gather and share information with the Safeguarding Children Partnership in order that its statutory function can be discharged regarding LCSPR's.

### **When not to seek consent**

There are a limited number of circumstances where professional **should not** seek consent.

e.g. where to do so would:

- Place a child at increased risk of significant harm
- Prejudice the prevention or detection of a serious crime
- Lead to unjustified delay in making enquiries about allegations of significant harm.



If a professional shares information without seeking consent, this should be clearly recorded, including the reasons for not seeking consent. Recording should set out the legal basis under which information is being shared.

It is important that all professionals who have contact with children and families are able to have conversations about consent. Not gaining consent where it is needed can cause delay in children and families accessing services that will help meet their needs.

### **1. Is there a clear and legitimate purpose to share the information?**

The following questions can be helpful in establishing whether there is a clear and legitimate purpose for sharing information.

Is there a legal basis or statutory duty for sharing the information? (e.g. s47 of the Children Act 1989 <sup>12</sup> or a court has made an order for certain information or files to be brought before the court), Is the request proportionate to the purpose for which disclosure is sought? Why is the information being shared or requested? Can either party, requesting or sharing the information, show a sufficient 'need to know'? Was the information obtained under a specific statutory power or duty which limits what can be done with it and who the information can be shared with? Will the request involve secondary disclosure? (Disclosure by the person to whom data has been disclosed to another agency or person e.g. if a GP provides data to a school and the school passes it to Children's Social Care).

- Is there another way to achieve the objective with less impact on confidentiality? (e.g. would anonymous data suffice?)

### **2. Does the information enable a person to be identified?**

- In most cases where information is shared at an operational level it will be about a named child. It may also identify others, such as a parent, carer or other family members.
- However, there will be other scenarios where anonymised information will be sufficient. For example, anonymised data may suffice for the purpose of data analysis or report writing. - The SCSP maintains a multi-agency dataset, which supports in gaining assurance around the safeguarding system, practices and the outcomes achieved for children across in Sandwell. This includes a range of anonymised and aggregated data from across partners, as data which personally identifies the individuals involved is not necessary to undertake the required analysis.
- If the information is anonymised, it can lawfully be shared as long as the purpose is legitimate. If the information allows a child and others to be identified, it is subject to data protection law and professionals must follow this Protocol and where appropriate take legal advice in deciding whether or not to share the information.

### **3. Is the information confidential?**

---

<sup>12</sup> <https://www.legislation.gov.uk/ukpga/1989/41/contents>

- Confidential information is information of some sensitivity, which is not already lawfully in the public domain or readily available from another public source, and which has been shared in a relationship where the person giving the information understood that it would not be shared with others.
- There is a common law duty of confidentiality when dealing with sensitive personal data. A breach of confidence will not occur if there is a recorded legitimate purpose to share, or if there is evidenced that freely given, explicit informed consent has been obtained.

#### 4. **If the information is confidential, has consent to share been obtained?**

- Consent must be freely given, informed and explicit. This means that the person giving consent needs to understand why information needs to be shared, who will see their information, the purpose for which it will be used and the implications of sharing that information.
- The ICO provides further guidance on what is meant by 'consent'<sup>13</sup>.
- Professionals need to consider whose consent should be sought. Where there is a duty of confidence, it is owed to a person who has provided the information on the understanding it is to be kept confidential and, in the case of medical or other records, the person to whom the information relates.
- The law does not set out a specific age at which children should be asked for consent. A young person aged 16 or 17, or a child under 16 who has the capacity to understand and make their own decisions, may give (or refuse) consent to sharing.
- In most cases, where a child cannot consent, or where a professional judge that they are not competent to consent, a person with parental responsibility should be asked to consent on behalf of the child. However, the capacity of the parent to consent also needs to be taken into consideration.

Professionals should refer to the Mental Capacity Act 2005<sup>14</sup> and their own agency or sector specific guidance in determining capacity to consent. If there is any doubt, or in case where there is conflict between the wishes of the parent and the child or two adults with parental responsibility, then professionals should seek guidance from their safeguarding lead.

- When a professional seeks consent for information to be shared, the following information should be provided as a minimum:
  - What information has been or will be collected
  - The purposes for which it will be used
  - Who the information might be shared with
  - The purposes for which the agencies that receive the information might use it (including detection of crime).

---

<sup>13</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/>

<sup>14</sup> <https://www.legislation.gov.uk/ukpga/2005/9/contents>

- The need to renew consent should be reviewed and professionals should be aware that individuals have the right to withdraw consent after they have given it.
- All sharing of sensitive information, even where there is consent, should be recorded including the legal basis for sharing information and the decision-making process for deciding that information should be shared.

**5. If consent has been refused, or there are good reasons not to seek consent to share confidential information, is there a sufficient public interest to share information?**

- Even where sharing of confidential information is not authorised, professionals may lawfully share it if this can be justified in the public interest. A public interest can arise in a range of circumstances e.g. to protect children or other people from harm, to promote the welfare of children or to prevent crime and disorder. In making a decision about whether there is sufficient public interest to share information, professionals must weigh up what might happen if the information is shared against what might happen if it is not, and make a decision based on a reasonable judgement.
- Where there is a clear risk of significant harm to a child, the public interest test will almost certainly be satisfied. There will be other cases where professionals will be justified in sharing some confidential information in order to make decisions on sharing further information or taking action - the information shared in such circumstances should be proportionate.
- Circumstances in which sharing confidential information without consent will normally be justified in the public interest are:
  - When there is evidence that the child has suffered, or is likely to suffer, significant harm
  - Where there is reasonable cause to believe that a child has suffered, or is likely to suffer, significant harm
  - To prevent significant harm arising to children, including through the prevention, detection and prosecution of serious crime (serious crime means any crime which causes or is likely to cause significant harm to a child or serious harm to an adult).
- In deciding whether the public interest justifies disclosing confidential information without consent, professionals should be able to seek advice from a line manager or designated safeguarding lead.
- If professionals decide to share confidential information without consent, this should be explained to the child or their parent, unless to do so would put the child at risk of harm.
- Professionals must record the context in which the information was shared, the legal basis for sharing information the perceived level of risk of harm at the time, the data requested, the data shared and with whom. Agencies may have a standard form for this or ensure that there is a signed and dated entry in the case notes.

## **6. If the decision is to share, is the right information being shared in the right way?**

If the decision is to share, professionals should share information in an appropriate way. This means:

- Share the information which is necessary for the purpose for which it is being shared
- Share the information with the person or people who need to know
- Check that the information is accurate and up-to-date
- Share it in a secure way
- Establish with the recipient whether they intend to pass it on to other people
- Ensure they understand the limits of any consent which has been given
- Inform the person to whom the information relates, and, if different, any other person who provided the information, if professionals have not already and it is safe to do so.

## **7. Have the decision and the reasons for sharing, or not sharing information been recorded?**

Professionals should record all decisions whether or not to share information and why. If the decision is to share, the record should include what information was shared and with whom, and who gave consent (dated and timed).

### **APPENDIX 3**

#### **Seven Golden Rules for Information Sharing**

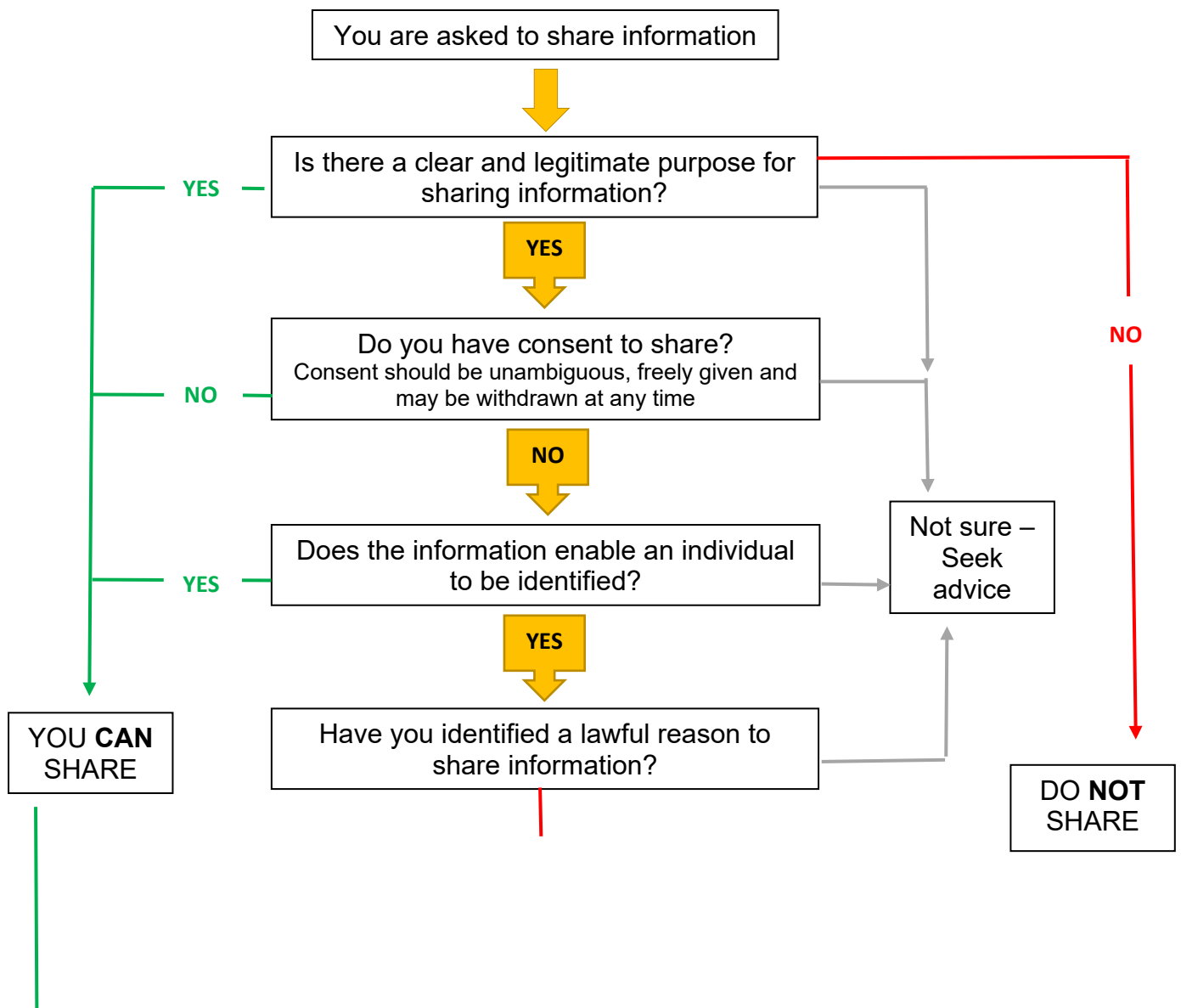
1. Remember that the Data Protection Act 2018 and human rights law are not barriers to justified information sharing but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) 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. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with informed 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, there is good reason 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 certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.

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.
6. Necessary, proportionate, relevant, adequate, 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 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.

(Taken from HM Government Statutory Guidance on Information Sharing)

#### APPENDIX 4

##### Flowchart of when and how to share information



————— NO —————→

- Share information:

  - Identify how much information to share.
  - Distinguish fact from opinion.
  - Ensure that you are giving the right information to the right person.
  - Ensure you are sharing the information securely.
  - Inform the person that the information has been shared if they were not aware of this and it would not create or increase risk of harm.

Record your information sharing decision and your reasons in line with your organisation policy.

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

Notes: Flowchart adapted from [HM Government \(2018\) Information Sharing Advice for practitioners providing safeguarding services to children, young people, parents and carers](#))

## APPENDIX 5

### SIGNATORIES TO THIS PROTOCOL

Organisation	Name	Position	Signature	Date
<b>Statutory Safeguarding Partners</b>				
SMBC				
SCT				
WMP				
CCG				
<b>Independent</b>				
Chair				
Scrutineer				
<b>SCSP Relevant Partners/Agencies</b>				
Education				