



Cheshire East Safeguarding  
Children's Partnership

Cheshire East Safeguarding Children's Partnership



Cheshire West and Chester Safeguarding Children's Partnership



Halton Children and Young People Safeguarding Partnership



Warrington Safeguarding Partnership

# Pan-Cheshire Safeguarding Children's Procedures

## Information Sharing Guidance

Advice for practitioners providing safeguarding services to  
children, young people, parents and carers

## Contents

<b>1. Introduction</b> .....	<b>3</b>
Who is the advice for? .....	3
<b>2. The Legal Basis for Information Sharing</b> .....	<b>4</b>
The Children Act 2004 .....	4
The GDPR and Data Protection Act 2018 .....	5
Article 8, European Convention on Human Rights.....	6
The Education Act 2002 .....	6
The Crime and Disorder Act 1998 Section 115 .....	7
Health and Social Care (Safety and Quality) Act 2015.....	7
The Local Government Act 1972 .....	7
The National Health Service Act 2006 .....	7
The Mental Capacity Act 2005 .....	7
The Care Act 2014 .....	8
<b>3. Other considerations</b> .....	<b>8</b>
The Common Law Duty of Confidentiality .....	8
Public Interest .....	8
The Domestic Violence Disclosure Scheme: .....	8
Child Sex Offender Disclosure Scheme.....	9
Age Assessment Information Sharing - Unaccompanied Asylum-Seeking Children.....	9
Caldicott Guardian Principles: .....	10
<b>4. Being alert to signs of abuse and neglect and taking action</b> .....	<b>11</b>
<b>5. Sharing information</b> .....	<b>11</b>
What constitutes consent? .....	12
The seven golden rules to sharing information .....	12
The Principles .....	13
When and how to share information.....	14
Sharing information securely .....	15
Flowchart on when and how to share information.....	16
<b>6. Myth-busting guide to information sharing</b> .....	<b>17</b>
<b>7. Useful resources and external organisations</b> .....	<b>17</b>
Other relevant departmental advice and statutory guidance .....	17

## 1. Introduction

Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious child safeguarding cases, where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe.

This guidance is based on [Information Sharing](#) (2018) and [Working together \(2018\)](#) HM Government and has been produced to support practitioners in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being. The guidance also reflects the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

This guidance does not deal in detail with arrangements for bulk or pre-arranged sharing of personal information between IT systems or organisations other than to explain their role in effective information governance.

### Who is the advice for?

This advice is for all frontline practitioners and senior managers working with children, young people, parents and carers who have to make decisions about sharing personal information on a case by case basis. Effective information-sharing underpins integrated working and is a vital element of both early intervention and safeguarding. Research and experience have shown repeatedly that keeping children safe from harm requires professionals and others to record, analyse, understand the significance of and share information about:

- A child's health and development, and exposure to possible harm;
- A parent who may need help, or may not be able to care for a child adequately and safely; and
- Those who may pose a risk of harm to a child.

When professionals share information at an early stage, this can reduce the risk of significant harm to children. Often, it is only when information from a number of sources has been shared and is then put together, that it becomes clear that a child has suffered, or is likely to suffer, significant harm.

Professionals providing services to both adults and children, for example GP's, may be concerned about the need to balance their duties to protect children from harm with their general duty of care towards their patient or service user, e.g. a parent. Some professionals face the added dimension of being involved in caring for or supporting more than one family member - the abused child, siblings, and an alleged abuser. However, in English Law, where there are concerns that a child is, or may be, at risk of significant harm, the overriding consideration is to safeguard the child. (Children Act 1989).

Practitioners should use their judgement when making decisions on what information to share and when and should consider this guidance, follow their own internal procedures or consult with their manager if in doubt. The most important consideration is whether sharing information is likely to safeguard and protect a child.

## 2. The Legal Basis for Information Sharing

All agencies that work with children and families share a commitment to safeguard and promote their welfare. For many agencies this is underpinned by a statutory duty or duties. This document briefly explains the legislation most relevant to work to safeguard and promote the welfare of children.

### The Children Act 2004

[Section 11](#) of the Children Act 2004 places duties on a range of organisations, agencies and individuals to ensure their functions, and any services that they contract out to others, are discharged having regard to the need to safeguard and promote the welfare of children, it places a duty on:

- Local authorities and district councils that provide children's and other types of services, including children's and adult social care services, public health, housing, sport, culture and leisure services, licensing authorities and youth services;
- NHS organisations and agencies and the independent sector, including NHS England and clinical commissioning groups, NHS Trusts, NHS Foundation Trusts and General Practitioners;
- The police, including police and crime commissioners and the chief officer of each police force in England and the Mayor's Office for Policing and Crime in London;
- The British Transport Police;
- The National Probation Service and Community Rehabilitation Companies;
- Governors/Directors of Prisons and Young Offender Institutions (YOIs);
- Directors of Secure Training Centres (STCs);
- Principals of Secure Colleges;
- Youth Offending Services (YOS).

Under [Section 10](#) of the same Act, the local authority is under a duty to make arrangements to promote co-operation between itself and organisations and agencies to improve the wellbeing of local children. This co-operation should exist and be effective at all levels of an organisation, from strategic level through to operational delivery. These organisations and agencies should have in place an array of arrangements that reflect the importance of safeguarding and promoting the welfare of children inclusive of:

Arrangements which set out clearly the processes for sharing information, with other practitioners and with safeguarding partners

### Safeguarding Children's Partnership (SCP)

The SCP replaces Local Safeguarding Children Board. This is because the law changed in the [Children and Social Work Act 2017](#). The statutory guidance on how the new safeguarding arrangements should work and be delivered are outlined in [Working Together to Safeguard Children 2018](#).

These new arrangements have been determined by the three key safeguarding partners – Children’s Services (Cheshire East, Cheshire West & Chester, Halton and Warrington), Cheshire Constabulary and NHS Cheshire Clinical Commissioning Group. All three safeguarding partners have equal and joint responsibility for the local safeguarding arrangements and to promote the welfare of all children in a local area.

The SCP is responsible for ensuring information is appropriately shared between and within partner organisations, addressing any barriers to information sharing and enabling a culture of appropriate information sharing supported as necessary by multi-agency training.

## **The GDPR and Data Protection Act 2018**

[The GDPR and Data Protection Act 2018](#) introduces new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information, it is important that accountability is defined to ensure that teams know who is responsible for making decisions and that actions taken are in the best interest of the child.

The GDPR and Data Protection Act 2018 place duties on organisations and individuals to process personal information fairly and lawfully placing a greater significance on organisations being transparent and accountable in their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing and sharing information securely ensuring it is only disclosed in appropriate circumstances and that it’s accurate, relevant and not held longer than necessary.

The Act balances the rights of the information subject and the need to share information about them. Never assume sharing is prohibited - it is essential to consider this balance in every case. [The Information Commissioner](#) published a statutory code of practice on information sharing to help adopt good practice.

All organisations should have arrangements in place, which set out clearly the processes and the principles for sharing information internally. In addition, these arrangements should cover sharing information with other organisations and practitioners, including third party providers to which local authorities have chosen to delegate children’s social care functions, and any Local Safeguarding Partners.

The GDPR and Data Protection Act 2018 is not a barrier to sharing information, where the failure to do so would cause the safety or well-being of a child to be compromised.

To effectively share information:

all practitioners should be confident of the lawful bases and processing conditions under the Data Protection Act 2018 and the GDPR which allow them to store and share information including information which is considered sensitive, such as health data, known under the data protection legislation as 'special category personal data'

where practitioners need to share special category personal data, for example, where information obtained is sensitive and needs more protection, they should always consider and identify the lawful basis for doing so under Article 6 of the GDPR, and in addition be able to meet one of the specific conditions for processing under Article 9. In effect, the Data Protection Act 2018 contains 'safeguarding of children and individuals at risk' as a processing condition that allows practitioners to share information, including without consent (where in the circumstances consent cannot be given, it cannot be reasonably expected that a practitioner obtains consent or if to gain consent would place a child at risk). However, practitioners should be mindful that a data protection impact assessment for any type of processing which is likely to be high risk must be completed, and therefore aware of the risks of processing special category data

Information **can be shared legally without consent** if a practitioner is unable, or cannot be reasonably expected, to gain consent from the individual or if to gain consent could place a child at risk.

Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental or emotional well-being.

## **Article 8, European Convention on Human Rights**

[Article 8](#) of The European Convention on Human Rights states that everyone has the right to respect for his/her private and family life, home and correspondence;

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others.

The GDPR and Data Protection Act 2018 place duties on organisations and individuals to process personal information fairly and lawfully; they are not a barrier to sharing information, where the failure to do so would cause the safety or well-being of a child to be compromised. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

## **The Education Act 2002**

[Section 175](#) of the [Education Act 2002](#) requires governing bodies of maintained schools and Further Education colleges to make arrangements to ensure that their

functions are carried out with a view to safeguarding and promoting the welfare of children.

Regulations made under [Section 157](#) state that proprietors of independent schools (which include Academies and Free schools) must make arrangements to safeguard and promote the welfare of pupils and in doing so must have regard to any statutory guidance issued by the Secretary of State. The Education (Non-Maintained Special Schools) (England) Regulations 2011 require non-maintained special schools to have arrangements for safeguarding and promoting the health, safety and welfare of the registered pupils at the school, and to have regard to this guidance.

### **The Crime and Disorder Act 1998 [Section 115](#)**

The power to disclose information is central to the Act's partnership approach. The Police have an important general power under common law to disclose information for the prevention, detection and reduction of crime. However, some other public bodies that collect information may not previously have had power to disclose it to the Police and others. This section puts beyond doubt the power of any organisation to disclose information to Police authorities, local authorities, Probation Service, Health Authorities, or to persons acting on their behalf, so long as such disclosure is necessary or expedient for the purposes of crime prevention. These bodies also have the power to use this information.

### **Health and Social Care (Safety and Quality) Act 2015**

[Section 3](#) of the [Health and Social Care \(Safety and Quality\) Act 2015](#) – A legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual.

### **The Local Government Act 1972**

The Local Government Act [Section 111\(1\)](#) – a local authority shall have the power to do anything which is calculated to facilitate, or is conducive to or incidental to, the discharge of any of their statutory functions.

The Local Government Act 2000 [Section 2\(1\)](#) – a local authority shall have the power to do anything which they consider is likely to achieve the promotion or improvement of social well-being of their area.

### **The National Health Service Act 2006**

[Section 82](#) of [The National Health Service Act 2006](#) – in exercising their respective functions NHS bodies and local authorities must co-operate with one another to secure and advance the health and welfare of the people of England and Wales.

[Section 201\(3\)\(d\)](#) – a disclosure of information may be made if it is for the purposes of criminal investigations or proceedings.

[Section 201\(6\)](#) – information to which this section applies may be disclosed in accordance with Section 201(3) despite any obligation of confidence that would otherwise prohibit or restrict the disclosure.

### **The Mental Capacity Act 2005**

When sharing information in respect of adults who lack the capacity to provide any required consent, information should only be shared when it is permitted by relevant legislation and if considered to be in the person's best interests.



Additionally, where a person lacks mental capacity to decide about their own personal information, the [Mental Capacity Act Code of Practice](#) states that certain other people may be able to request access to that information. This would be somebody with a lasting power of attorney, an enduring power of attorney or who is a deputy appointed by the Court of Protection.

The [Principals, Section 1](#) of the [Mental Capacity Act 2005](#) states that a person must be assumed to have capacity unless there is evidence that they are not able to make the relevant decision. Mental capacity is assessed in relation to the particular decision which needs to be made. This means that whether a young person has mental capacity to make a particular decision or not has to be considered on an individual basis in the light of the circumstances at the time. You cannot just say that someone lacks mental capacity generally.

## **The Care Act 2014**

[Transition for children to adult care and support \(Sections 59-66\)](#) addresses the child's capacity to consent to a child's needs assessment being undertaken where the child does not consent, or where the child lacks capacity to consent but the authority is satisfied that carrying out a child's needs assessment would be in the child's best interests.

## **3. Other considerations**

### **The Common Law Duty of Confidentiality**

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent. Legal precedent states that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. You cannot use or share information which was originally provided in confidence without the individual's permission unless there is an overriding reason in the public interest for this to happen or another law or power permits disclosure.

### **Public Interest**

The relevant issues for professionals usually concern sharing information where consent has been withheld. Even where you do not have consent to share confidential information, you may lawfully share it if this can be justified in the public interest. The public interest threshold is not necessarily difficult to meet - particularly in emergency situations. As is the case for all personal information processing, initial thought should be given as to whether the objective can be achieved by limiting the amount of information shared - does all of the personal information need to be shared to achieve the objective? Where there is a clear risk of significant harm to a child, or serious harm to adults, the public interest test will almost certainly be satisfied.

### **The Domestic Violence Disclosure Scheme:**

The Domestic Violence Disclosure Scheme (DVDS) commenced on 8 March 2014. The DVDS gives members of the public a formal mechanism to make enquires about an individual who they are in a relationship with, or who is in a relationship with someone they know, where there is a concern that the individual may be violent towards their partner. This scheme adds a further dimension to the information sharing



about children where there are concerns that domestic violence and abuse is impacting on the care and welfare of the children in the family.

Members of the public can make an application for a disclosure, known as the 'right to ask'. Anybody can make an enquiry, but information will only be given to someone at risk or a person in a position to safeguard the victim. The scheme is for anyone in an intimate relationship regardless of gender.

Partner agencies can also request disclosure is made of an offender's past history where it is believed someone is at risk of harm. This is known as 'right to know'. If a potentially violent individual is identified as having convictions for violent offences, or information is held about their behaviour which reasonably leads the Police and other agencies to believe they pose a risk of harm to their partner, a disclosure will be made.

### **Child Sex Offender Disclosure Scheme**

The Child Sex Offender Disclosure (CSOD) Scheme is designed to provide members of the public with a formal mechanism to ask for disclosure about people they are concerned about, who have unsupervised access to children and may therefore pose a risk. This scheme builds on existing, well established third-party disclosures that operate under the Multi-Agency Public Protection Arrangements (MAPPA).

Police will reveal details confidentially to the person most able to protect the child (usually parents, carers or guardians) if they think it is in the child's interests. The scheme has been operating in all 43 Police areas in England and Wales since 2010. The scheme is managed by the Police and information can only be accessed through direct application to them.

If a disclosure is made, the information must be kept confidential and only used to keep the child in question safe. Legal action may be taken if confidentiality is breached. A disclosure is delivered in person (as opposed to in writing) with the following warning:

If the person is unwilling to sign the undertaking, the Police must consider whether the disclosure should still take place.

- That the information must only be used for the purpose for which it has been shared i.e. in order to safeguard children;
- The person to whom the disclosure is made will be asked to sign an undertaking that they agree that the information is confidential and they will not disclose this information further;
- A warning should be given that legal proceedings could result if this confidentiality is breached. This should be explained to the person and they must sign the undertaking' (Home Office, 2011, p16).

### **Age Assessment Information Sharing - Unaccompanied Asylum-Seeking Children**

The issue of age assessment in social work with asylum seeking young people remains controversial and has been something that Children's social care have struggled with since the millennium. The ADCS Asylum Task Force has worked with the Home Office to provide two new jointly agreed documents, as detailed below. The ADCS guidance contains practical advice on preparing for, and conducting, age assessments, as well as a range of useful resources covering issues such as trafficking, trauma and memory, and legislation and case law. *The use of the proforma and consent form is voluntary. The content does not, nor does it seek to, be binding on local authorities. It is simply a recommended approach.*

- [Introduction to Joint Working Guidance](#)
- [Age Assessment Information Sharing for Unaccompanied Asylum-Seeking children: Explanation and Guidance](#)
- [Joint Working Guidance](#)
- [Age Assessment Information Sharing Proforma](#)

### **Caldicott Guardian Principles:**

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that the NHS, Local Authority Social Services Departments and partner organisations satisfy the highest practicable standards for handling patient identifiable information.

### **The Seven Caldicott Principles**

1. Justify the purpose(s) for using confidential information;

2. Use confidential information only when it is necessary;

3. Use the minimum necessary confidential information;

4. Access to confidential information should be on a strict need-to-know basis;

5. Everyone with access to personal confidential data should be aware of their responsibilities;

6. Comply with the law;

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

8. Inform patients and service users about how their confidential information is used

These are applicable to Local Authorities and Health Trusts. They have more recently been extended into councils with social care responsibilities, in order to provide a framework for working within the Data Protection Act 2018 and to promote appropriate information sharing. Every local Health Service and Local Authority has its own Caldicott Guardian, to provide advice and guidance on appropriate information sharing.

## 4. Being alert to signs of abuse and neglect and taking action

All practitioners should be alert to the signs and triggers of [child abuse and neglect](#). Abuse (emotional, physical and sexual) and neglect can present in many different forms. Indicators of abuse and neglect may be difficult to spot.

Children may disclose abuse, in which case the decision to share information is clear, as actions must be taken to respond to the disclosure. In other cases, for example, neglect, the indicators may be more subtle and appear over time.

In these cases, decisions about what information to share, and when, will be more difficult to judge. Everyone should be aware of the potential for children to be sexually exploited for money, power or status, and individuals should adopt an open and inquiring mind to what could be underlying reasons for behaviour changes in children of all ages.

If a practitioner has concerns about a child's safety or welfare, they should share the information with Children's Social Services and/or Cheshire Constabulary. For more information see:

<https://www.proceduresonline.com/pancheshire>

Security of information sharing must always be considered and should be proportionate to the sensitivity of the information and the circumstances. If it is thought that a crime has been committed and/or a child is at immediate risk, the police should be notified immediately.

## 5. Sharing information

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right services at the right time and prevents a need from becoming more acute and difficult to meet.

Poor or non-existent information sharing is a factor repeatedly identified as an issue in serious safeguarding cases carried out following the death of or serious injury to, a child. In some situations, sharing information can be the difference between life and death.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing information they hold and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.

[Professor Munro's review of child protection](#) concluded the need to move towards a child protection system with less central prescription and interference, where we place greater trust in, and responsibility on, skilled practitioners at the frontline. Those skilled practitioners are in the best position to use their professional judgement about when to share information with colleagues working within the same organisation, as well as with those working within other organisations, in order to provide effective early help, to promote their welfare, and to keep children safe from harm.

[Lord Laming](#) emphasised that the safety and welfare of children is of paramount importance and highlighted the importance of practitioners feeling confident about when and how information can be legally shared. He recommended that all staff in

every service from frontline practitioners to managers in statutory services and the voluntary sector should understand the circumstances in which they may lawfully share information, and this it is in the public interest to prioritise the safety and welfare of children.

### What constitutes consent?

The UK GDPR sets a high standard for consent to share information, and requires that it must be specific, time limited and able to be withdrawn. Consent is a lawful basis under which information can be **shared in UK GDPR**. and would cover sharing where the individual has given clear consent for you to process their personal data for a specific purpose; e.g. provision of Early **help services**.

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement. Consent is one lawful basis for processing information, but there are five others. You must always choose the lawful basis that most closely reflects the true nature of your relationship with the individual and the purpose of the processing

The UK GDPR does not contain specific provisions on capacity to consent, but issues of capacity are bound up in the concept of 'informed' consent. Generally, you can assume that adults have the capacity to consent unless you have reason to believe the contrary. However, you should ensure that the information you provide enables them to be fully informed.

### The seven golden rules to sharing information

The general principle is that information will only be shared with the consent of the subject of the information.

However, there are circumstances when sharing confidential information without consent can be justified in the public interest, for example seeking consent would be inappropriate or unsafe

1	Remember that the GDPR, 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 (via a privacy notice), and seek their agreement, unless it is unsafe or inappropriate to do so.
3	Seek advice from other practitioners, or your information governance lead if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4	Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you

	do not have consent, be mindful that an individual might not expect information to be shared.
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.

The 'Seven Golden Rules' will help support your decision making so you can be more confident that information is being shared legally and professionally. Each situation should be considered on a case-by-case basis.

If you continue to have concerns about whether to share information or not, seek advice from your manager or the Information Governance Team. The Information sharing guidance for Practitioners makes an important point which should be borne in mind; personal information can be held in many different ways, including case records or electronically in a variety of IT systems with access for different professionals. Information can be shared via email as well as by direct person to person contact. Remember that however the information is shared, it should always be recorded in the individual's record.

## The Principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations. Practitioners should use their judgement when making decisions about what information to share and should follow organisation procedures or consult with their manager if in doubt.

**The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.**

**Necessary and proportionate** - When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and Data Protection Act 2018 and you should consider the impact of disclosing information on the information subject and any third parties. Information must be proportionate to the need and level of risk.

**Relevant** - Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

**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.

**Accurate** - Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

**Timely** - Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

**Secure** - Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

**Record** - Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

## **When and how to share information**

When asked to share information, you should consider the following questions to help you decide if, and when, to share. If the decision is taken to share, you should consider how best to effectively share the information. A flowchart follows the text.

### When

Is there a clear and legitimate purpose for sharing information?

- Yes – see next question
- No – do not share

Do you have consent to share?

- Yes – you can share but should consider how
- No – see next question

Does the information enable an individual to be identified?

- Yes – see next question
- No – you can share but should consider how

Have you identified a lawful reason to share information without consent?

- Yes – you can share but should consider how
- No – do not share

### How

- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right individual

- Ensure where possible that you are sharing the information securely
- Where possible, be transparent with the individual, informing them that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual.

All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage, you are unsure about how or when to share information you must seek advice on this. You should also ensure that the outcome of the discussion is recorded.

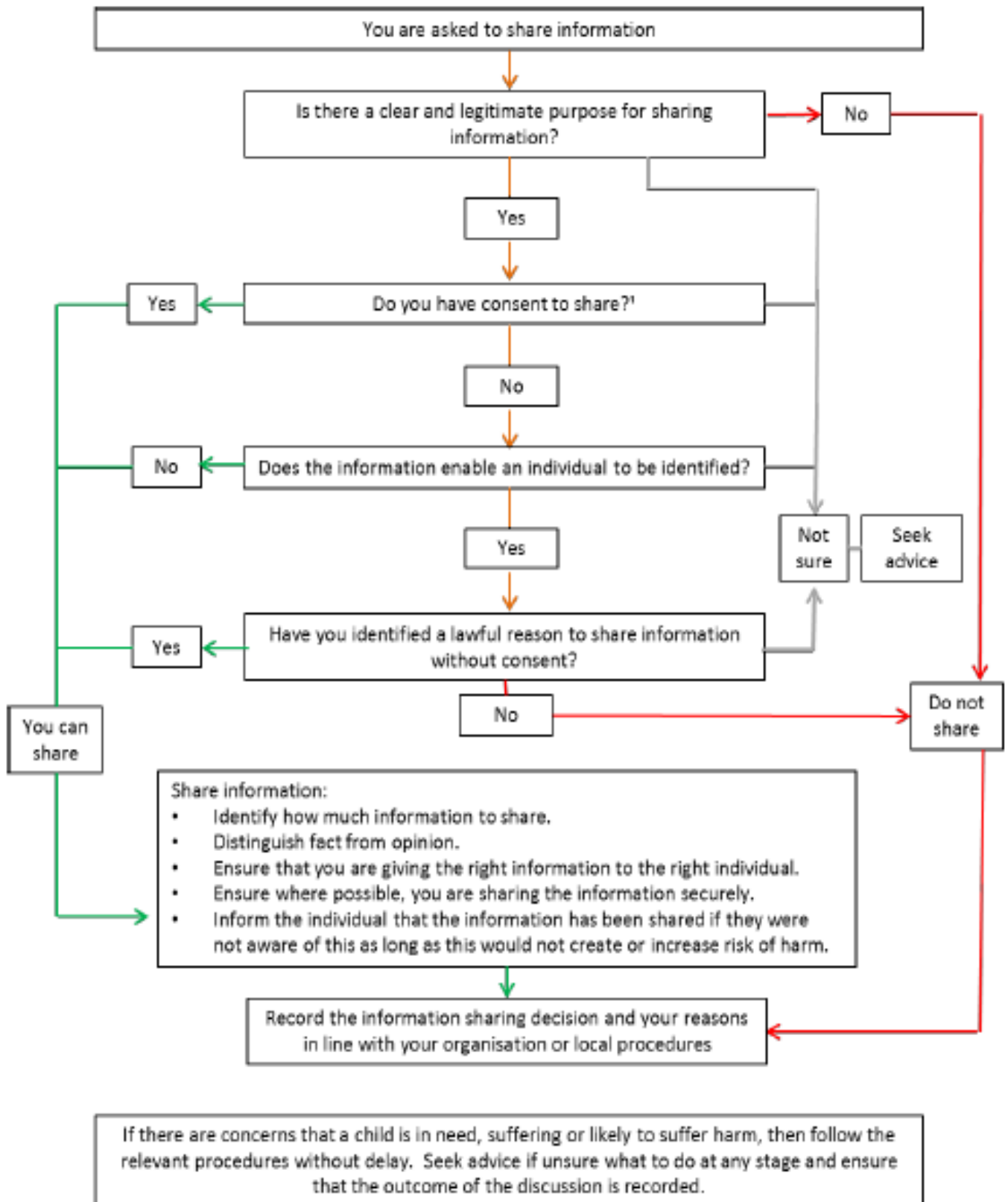
### **Sharing information securely**

When you share information, whatever the method, you must take precautions to ensure the sharing is as secure as possible. Here are some tips;

- **Face-to-face in meetings** – consider whether everyone present ‘needs to know’ and are legally entitled to hear or receive the information you share.
- **Discussions in offices or public places** – be careful not to identify people by names unless you have to and choose places where you cannot be overheard by those who shouldn’t hear your discussions.
- **Sharing over telephone** – check the person’s identity and entitlement to the information before you release it.
- **Sharing by fax or letter** – you must double check the recipient’s fax number/ name and address details before you send it. Contact the recipient to ensure they are waiting by the fax machine and ask them to confirm they have received the document(s)
- **Sharing by email** – you must follow council guides to sharing information securely by email. Personal information must not be emailed unless the information is encrypted, or the sender and recipient have a ‘secure email address’.



## Flowchart on when and how to share information



1. Consent must be unambiguous, freely given and may be withdrawn at any time

## 6. Myth-busting guide to information sharing

Sharing information enables practitioners and agencies to identify and provide appropriate services that safeguard and promote the welfare of children. Below are common myths that may hinder effective information sharing.

### **Data protection legislation is a barrier to sharing information**

No – the Data Protection Act 2018 and GDPR do not prohibit the collection and sharing of personal information, but rather provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them.

### **Consent is needed to share personal information**

No – you do not need consent to share personal information. It is one way to comply with the data protection legislation but not the only way. The GDPR provides a number of bases for sharing personal information. It is not necessary to seek consent to share information for the purposes of safeguarding and promoting the welfare of a child provided that there is a lawful basis to process any personal information required. The legal bases that may be appropriate for sharing data in these circumstances could be 'legal obligation', or 'public task' which includes the performance of a task in the public interest or the exercise of official authority. Each of the lawful bases under GDPR has different requirements.<sup>15</sup> It continues to be good practice to ensure transparency and to inform parent/ carers that you are sharing information for these purposes and seek to work cooperatively with them.

### **Personal information collected by one organisation/agency cannot be disclosed to another**

No – this is not the **case unless** the information is to be used for a purpose incompatible with the purpose for which it was originally collected. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners<sup>16</sup>.

### **The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information**

No – this is not the case. In addition to the Data Protection Act 2018 and GDPR, practitioners need to balance the common law duty of confidence and the Human Rights Act 1998 against the effect on individuals or others of not sharing the information.

### **IT Systems are often a barrier to effective information sharing**

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful for information sharing. IT systems are most valuable when practitioners use the shared data to make more informed decisions about how to support and safeguard a child.

## 7. Useful resources and external organisations

- [The Information Commissioners Office \(ICO\) website](#)
- [Practice guidance on sharing adult safeguarding information](#)

### **Other relevant departmental advice and statutory guidance**

- [Working Together to Safeguard Children \(2018\)](#)

- [Keeping Children Safe in Education \(2020\)](#)
- [What to do if you are worried a child is being abused \(2015\)](#)