**Information Sharing and Consent 1 Minute Guide**

This 1 Minute Guide provides a summary of the key facts related to Information Sharing and Consent.

1. **Introduction**

Data protection law is not a barrier to sharing information when it is necessary, proportionate, and justified to do so. The most important consideration is to safeguard and promote the welfare of the child or young person.

[Working Together 2023](https://assets.publishing.service.gov.uk/media/65803fe31c0c2a000d18cf40/Working_together_to_safeguard_children_2023_-_statutory_guidance.pdf) is the statutory guidance for “inter-agency working to safeguard and promote the welfare of children”. It states

*“practitioners should be proactive in sharing information as early as possible to help identify, assess and respond to risks or concerns about the safety and welfare of children, whether this is when problems are first emerging, or where a child is already known to local authority children’s social care”*

(2023:18 Paragraph 28)

Practitioners are responsible for lawfully sharing the information they hold and must not assume that someone else will pass on information that may be critical to safeguard and promote the welfare of a child.

Practitioners should use their judgement when making decisions about what information to share and must follow [organisational procedures](https://swcpp-devon.trixonline.co.uk/chapter/information-sharing#the-uk-general-data-protection-regulation-uk-gdpr-and-the-data-protection-act-2018) or consult with their manager, [information governance](mailto:keepdevonsdatasafe@devon.gov.uk) or [data protection officer](https://inside.devon.gov.uk/task/gdpr/contact-the-data-protection-officer/) if in doubt.

When sharing information, practitioners must ensure it is:

* Necessary and proportionate to the circumstances;
* Relevant to the circumstances;
* Adequate and sufficient for its purpose;
* Accurate and up to date;
* Timely, particularly in an emergency;
* Exchanged securely; and

1. **Sharing of Information**

Professionals sharing information about a child DO NOT REQUIRE consent if the sharing of information is to ‘**safeguard and promote the welfare of the child’**.

Working Together (2023:161) defines safeguarding and promoting the welfare of a child as:

* Protecting children from maltreatment, whether the risk of harm comes from within the child’s family and/or outside (from the wider community), including online.
* Preventing impairment of children’s mental and physical health or development;
* Ensuring that children are growing up in circumstances consistent with the provision of safe and effective care;
* Taking action to enable all children to have the best outcomes.

While consent is **NOT** required to share information to safeguard the welfare of the child, it is best practice for the family to be told of the intention to share the information unless to do so would place the child at immediate risk of harm.

## **Myth Busting Sharing Information (Working Together 2023:21)**

### **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. 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.

### **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.

1. **Consent for Intervention**

Consent means offering individuals real choice and control. The UK GDPR does not contain specific provisions on capacity to consent to intervention, but issues of capacity are bound up in the concept of 'informed' consent. Generally, you can assume that adults, and children aged 13 and over, have the capacity to consent unless you have reason to believe the contrary. You should ensure the information you provide enables them to be fully informed.

Interventions (which include an assessment of need) provided through Universal, Early Help services and Child in Need s.17 Children Act 1989, require consent from the family.

If the Front Door are refused consent and the child meets the threshold for Child in Need, the information is reviewed by a team manager to determine whether, without intervention, the child is suffering or likely to suffer significant harm (S.47 Children Act 1989).

Where a child is not considered at risk of significant harm and consent for intervention is not given, the family should be provided with full information about the benefits of assessment and support. Any refusal should be then accepted and recorded.

When consent cannot be confirmed either way, within 24 hours of the referral, the ‘need for assessment’ is transferred to Assessment & Intervention Team by the Front Door (See [Consent Withdrawn for Assessment practice guide)](https://devoncc.sharepoint.com/:w:/s/reSOURCEforChildrensSocialCare/PrincipalSWResources/EePykO6MCjlAje10t4snUpABLF-bdsU96JsCbFQjAN5lFw?e=C66K8F).

1. **Terminology**

**Data Controllers and Data Processors**

Your employer (local authority, health service, police, school etc) is what is known as a “Data Controller”. Data Controllers are required to demonstrate compliance with the data protection principles as well as the other UK GDPR requirements.

When sharing information, you will be doing so on behalf of your agency. It is important all practitioners ensure one of the legal bases for sharing information applies (see above) and that they abide by the principles for sharing information.

**Data Protection Impact Assessment (DPIA)**

A DPIA is usually only required if large amounts of information affecting many data subjects is being shared, not for individual episodes of information sharing. There may be occasions when there is a concern about sharing a specific piece of information in which case, practitioners should consult with their designated safeguarding lead and / or information governance lead to evaluate the privacy risks that may arise from sharing that information.

If a new DPIA is required or an existing one is revised, there is a legal requirement to seek the advice of your organisation’s data protection officer (See [**UK GDPR Article 35(2)**](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/)).

**Processing Data**

Processing information for the purposes of information sharing guidance simply means collecting, recording, accessing, sharing or otherwise making use of the information available to practitioners.

**Personal Data**

Personal data may be shared within the guidelines set out above. It includes information that would directly or indirectly identify an individual. There may also be other information about the person linked to the personal data, which would then also be personal data.

Personal data that has been “pseudonymised” (where details have been replaced with a key) or “de-identified” (where identifying details have been removed) can still be personal data – even if an indirect identification requires access to an additional database.

**Special Category Data**

Special category data is personal data, which is more sensitive and needs more protection such as, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes, health, sex life and sexual orientation.

Special category data can be shared so long as one of the conditions for processing special category data are met (See Article 9, UK GDPR) as well as the legal basis for processing. These include:

**Reasons of substantial public interest (Article 9(2)(g))** which includes the processing of information to prevent or detect unlawful acts, protecting the public and safeguarding of children and individuals at risk; and

**Health or Social Care (Article 9(2)(h))** which includes the processing of information for the purposes of preventive medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.