Information Sharing and Consent Legal Briefing Guidance Notes

This note is provided for information only and should not be relied upon as legal advice. Specific legal advice should be sought in any case where relevant issues arise.

The purpose of this briefing note is to cover the key aspects of information sharing and consent, to support local authorities and practitioners in securing sufficient and appropriate consent as part of the EHC process. The briefing will inform CDC's work with local authorities to develop templates, an FAQ and guidance on how best to secure appropriate consent from families. These should support both local authorities and practitioners to be confident in their consent processes, and to ensure that families are informed and can work in genuine partnership.

1. Consent is not always necessary for information to be shared – there may be other legitimate reasons to share information where consent has not or cannot be obtained, most obviously in a situation where there may be a significant risk of harm to a child.

2. It will however generally be necessary and appropriate to seek consent before personal information about a child or family member is shared.[1]

3. The relevant legal considerations in relation to information sharing include:

    a. The Data Protection Act 2018 and the General Data Protection Regulation (GDPR)[2]
    b. Article 8 of the European Convention on Human Rights (ECHR), which public bodies must act in accordance with under the Human Rights Act 1998
    c. The common law principle of confidentiality

1 See para 17 below re the 'Golden Rule' in the government guidance on information sharing; ''Where possible, share information with consent…'.

2 The ICO states that 'The GDPR came into effect on 25 May 2018. As a European Regulation, it has direct effect in UK law and automatically applies in the UK until we leave the EU (or until the end of any agreed transition period, if we leave with a deal). After this date, it will form part of UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.' See https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/

4. The Information Commissioner's Office (ICO) states[3] that 'The GDPR sets out seven key principles: Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and confidentiality (security); Accountability. These principles should lie at the heart of your approach to processing personal data.'

5. Under the DPA 2018 and the GDPR, it is essential to identify the lawful basis on which data is being processed. As the ICO states[4] , 'You must have a valid lawful basis in order to process personal data.[5] There are six available lawful bases for processing.[6] No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.'

6. The ICO also states that 'You must determine your lawful basis before you begin processing, and you should document it... Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.'

7. Furthermore 'If you are processing special category data[7] you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.'

8. The first lawful basis is 'consent'. The ICO states[8] that 'The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.' However note what is said below in the government guidance on information sharing as to the need to obtain consent where possible in the children's context.

9. The ICO states further that:

    a. 'Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
    b. Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
    c. Explicit consent[9] requires a very clear and specific statement of consent.
    d. Keep your consent requests separate from other terms and conditions.

---

3 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

4 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

5 'Personal data' simply means 'information about a particular living individual'; see https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

6 The ICO confirms (at link above) that 'Almost anything you do with data counts as processing; including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.'

7 See para 12 below.

8 ttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

9 See para 12 below re 'Special category data'.

e. Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
f. Be clear and concise.
g. Name any third party controllers[10] who will rely on the consent. [11]
h. Make it easy for people to withdraw consent and tell them how.
i. Keep evidence of consent – who, when, how, and what you told people.
j. Keep consent under review, and refresh it if anything changes.
k. Avoid making consent to processing a precondition of a service.
l. Public authorities and employers will need to take extra care to show that consent is freely given, and should avoid over-reliance on consent.'

10. Other potential legal bases for data processing are:

a. Legal obligation. The ICO states[12] that 'You can rely on this lawful basis if you need to process the personal data to comply with a common law or statutory obligation... The processing must be necessary. If you can reasonably comply without processing the personal data, this basis does not apply. You should document your decision to rely on this lawful basis and ensure that you can justify your reasoning. You should be able to either identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out your obligation.'

b. Public task. The ICO states[13] that 'You can rely on this lawful basis if you need to process personal data: 'in the exercise of official authority'. This covers public functions and powers that are set out in law; or to perform a specific task in the public interest that is set out in law... You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law. The processing must be necessary. If you could reasonably perform your tasks or exercise your powers in a less intrusive way, this lawful basis does not apply.

10 The ICO states that 'A controller is the person that decides how and why to collect and use the data. This will usually be an organisation, but can be an individual (eg a sole trader). If you are an employee acting on behalf of your employer, the employer would be the controller.' See https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/some-basic-concepts/

11 In this regard consideration needs to be given to whether any third parties have been sub-contracted as part of the EHCP process, as they will need to be identified if they want to rely on consent obtained by the LA. The ICO code of practice on data sharing contains the following case study: 'A council is outsourcing work previously carried out by its children and family services department to a charity. The charity will need details of the families currently receiving services to take over the council's role. The council writes to customers to tell them what is happening. As customers have no option but to deal with the new provider if they want to continue to receive their services, the council's letter should explain clearly who will be providing the service and what information will be passed over. It should reassure customers that information will continue to be used for the same purposes.' However note that this code of practice (available at https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf) is still to be updated to reflect the GDPR and the 2018 Act.

12 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/

13 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

Document your decision to rely on this basis to help you demonstrate compliance if required. You should be able to specify the relevant task, function or power, and identify its statutory or common law basis.'

11. As such where local authorities seek to rely on either the 'Legal obligation' or 'Public task' legal basis, they need to be clear on the statutory or common law basis of the duty (or potentially power) they are relying on as the basis for processing the data.

12. For 'special category data' (broadly similar to the previous concept of 'sensitive personal information'), you must also be able to identify a separate condition to justify processing, in addition to the appropriate lawful basis. Much of the data processed by local authorities in the context of EHC plans will include 'special category data'. The relevant conditions include:

    a. Explicit consent
    b. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of social protection law
    c. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
    d. Processing relates to personal data which are manifestly made public by the data subject
    e. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity[14]
    f. Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. NB - schedule 1 part 2 of the DPA 2018 contains specific 'substantial public interest' conditions.[15]
    g. Processing is necessary for the purposes of ...the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law...

13. Importantly, the information sharing guidance (see below) states that 'where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information without consent' (emphasis as original).

14 This may potentially be relevant where the processing is necessary to comply with Tribunal directions.

15 The ICO guidance on these provisions is forthcoming. It is important to note the general requirement in para 5 of the Schedule for an 'appropriate policy document' to be in place. As such local authorities should not seek to rely on the 'substantial public interest justification without taking specific legal advice. Note that under para 6 of the Schedule, processing which is necessary in 'the exercise of a function conferred on a person by an enactment or rule of law' and 'is necessary for reasons of substantial public interest' is justified (subject to the requirement above for an 'appropriate policy document'.

14. The ICO has published specific guidance on 'Children and the GDPR'.[16] The guidance includes:

a. 'The concept of competence (the child's capacity to understand the implications of their decisions) remains as valid under the GDPR as under the 1998 Act.

If a child is not competent to exercise their own data protection rights or consent to processing themselves then it will usually be in their best interests to allow an individual with parental responsibility to act on their behalf. If a child is competent then your overriding consideration should still be what is in their best interests however, in most cases it should be appropriate to let the child act for themselves.'

b. '…the GDPR requires the provision of age-appropriate privacy notices for children, and says that the right to have personal data erased is particularly relevant when processing is based upon the consent of a child.'

c. 'If you process children's personal data then you should think about the need to provide the specific protection required by Recital 38[17] from the outset and design your processing, products and systems with this mind. This is vital if you regularly or systematically process children's personal data. It is usually easier to incorporate child friendly design into a system or product as part of your initial design brief than to try and add it in later. We recommend that you use a Data Protection Impact Assessment (DPIA) to help you with this, and to assess and mitigate data protection risks to the child…'

d. 'If your processing is likely to result in a high risk to the rights and freedoms of children then you must do a [Data Protection Impact Assessment – DPIA] (emphasis added). The ICO has produced guidance on processing that it considers to be likely to result in a high risk to data subjects and therefore requires a DPIA.[18] The list includes the use of children's personal data for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.'

e. 'Transparency is also key. You can raise children's (and their parents') awareness of data protection risks, consequences, safeguards and rights by:

- telling them what you are doing with their personal data;
- being open about the risks and safeguards involved; and
- letting them know what to do if they are unhappy.

16 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/

17 Recital 38 to the GDPR includes 'Children require specific protection with regard to their personal data as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.'

18 See guidance from the ICO on DPIAs at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

This will also help them make informed decisions about what personal data they wish to share.'

f. 'As with any other processing, fairness and compliance with the data protection principles should lie at the heart of all your processing of children's personal data. The purpose of these principles is to protect the interests of the individuals and this is particularly important where children are concerned. They apply to everything you do with personal data (except where you are entitled to rely upon an exemption) and are key to complying with the GDPR.'

g. 'The concept of the best interests of the child comes from Article 3 of the United Nations Convention on the Rights of the Child. Although it is not specifically referenced in the GDPR it is something that the Commissioner will take into account when considering compliance, and that you should consider when making decisions about the processing of children's personal data.'

h. 'It is good practice to invite the views of children themselves when you are designing your processing, including diverse groups who can provide a range of feedback. This can help you to identify risks, design safeguards and assess understanding, as well as giving you an opportunity to test your system or product on the end user.

It is also consistent with the UN Convention on the rights of the child which provides at Article 12 that every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.'

i. 'There may be circumstances in which you wish to process a child's personal data using consent as your lawful basis for processing. This may be appropriate if you are truly able to give children (or their parents) informed choice and control over how you use their personal data. However consent shouldn't be used as a way of avoiding your own responsibility for assessing the risks inherent in the processing. Although consent is a lawful basis for processing children's personal data, using it does not necessarily guarantee that the processing is fair, and it isn't always the most appropriate basis.'

j. 'Where the child is not competent then, in data protection terms, their consent is not 'informed' and it therefore isn't valid. If you wish to rely upon consent in this situation, you need the consent of a person with parental authority over that child, unless it is evident that it would be against the best interests of the child to seek such parental consent.'

k. 'If you accept consent from a holder of parental responsibility over a child then you also need to think about how you let the child know that he or she has a right to withdraw that consent once they are competent to make such a decision. You should provide this information in any case as part of any privacy information directed at the child.

We would also recommend that you include it as part of any regular reminders you send to data subjects about their privacy settings and how to update them.'

l. 'If you want to share children's personal data with third parties then you need to follow the approach set out in our Data Sharing Code of Practice.[19] Although this has been issued under the Data Protection Act 1998 its basic approach remains valid under the GDPR. In time this guidance will be updated to reflect the specific provisions of the GDPR and the Data Protection Act 2018. We would also recommend that you carry out a DPIA to assess the risks inherent in the data sharing.

If the processing falls within one of the categories the Commissioner considers to be likely to result in a high risk to the rights and freedoms of children then a DPIA is compulsory.'

m. 'You must provide children with the same information about what you do with their personal data as you would give to adults. In order for processing to be fair, there is the same need for transparency, as this gives an individual control and choice.'

n. 'If you are relying upon parental consent then, in terms of ensuring that the consent is informed, it is the holder of parental responsibility rather than the child who needs to understand what they are consenting to.

Providing them with clear privacy information should meet this requirement. However… children do not lose their rights as data subjects to transparency just because consent has been given by a holder of parental responsibility. In practice this means that you need to give both the holder of parental responsibility and the child clear and accessible privacy information. Again you could achieve this by developing different versions for these different audiences, or by producing a child friendly version that can also be understood by parents.'

o. 'The Commissioner expects controllers whose services are used by very young children to develop privacy information that can be accessed by children as and when they develop the necessary level of understanding, or in conjunction with their parents. You should ensure that this is periodically brought to the child's attention throughout your ongoing processing relationship with them (for example when providing regular reminders about privacy settings).'

p. 'All data subjects, including children have the right to:

- be provided with a transparent and clear privacy notice which explains who you are and how their data will be processed…

19 https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. The data sharing code states on its front page 'This code has not been updated since the Data Protection Act 2018 became law. We are working on updating the code and have launched a call for views…'.

- be given a copy of their personal data;
- have inaccurate personal data rectified and incomplete data completed;
- exercise the right to be forgotten and have personal data erased…;
- restrict the processing in specified circumstances;
- …
- object to processing carried out under the lawful bases of public task or legitimate interests…'

15. Under Article 8 ECHR, processing of personal data is likely to be an 'interference' with the child and/or family member's right to respect for the private life (and / or their family life). That interference has to be 'justified' to avoid a human rights breach. Justification requires:

    a. A 'legitimate aim' – i.e. that the processing is being done for a proper process
    b. That the processing is proportionate to that aim – in other words that it is:

        i. Rationally connected to it;
        ii. No more than necessary to achieve the aim; and
        iii. Strikes a 'fair balance' between the rights of the relevant individuals and the wider public interest.

16. It would seem likely however that if a local authority complies with the requirements of the GDPR and the DPA 2018, it will avoid an unlawful interference with any person's Article 8 ECHR rights. This is because concepts of necessity and proportionality are built into the requirements of the GDPR and the DPA 2018.

17. The common law concept of confidentiality focuses on the need to obtain consent for the use of confidential information.

    A guide to confidentiality in health and social care published by the Health and Social Care Information Centre in September 2013[20] states that 'The key principle is that information confided should not be used or disclosed further, except as originally understood by the confider, or with their subsequent permission. Although judgements have established that confidentiality can be breached 'in the public interest', these have centred on case-by-case consideration of exceptional circumstances.'

18. It is important to keep in mind the government guidance, 'Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers', last updated in July 2018.[21]

20 Available at https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care

21 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721581/Information_sharing_advice_practitioners_safeguarding_services.pdf

The summary states as follows: '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 case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe.'

19. The first 'golden rule' is 'Remember that the General Data Protection Regulation (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.'

20. The fourth golden rule deals expressly with consent issues: '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.'

21. The guidance further states that 'The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.'

22. In addition, the guidance states that 'information can be shared legally without consent, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk' (emphasis as original).

23. With respect to confidentiality, the guidance says as follows:

'If information collection and sharing is to take place with the consent of the individuals involved, providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the Human Rights Act 1998'.

'If the information is confidential, and the consent of the information subject is not gained, then practitioners need to decide whether there are grounds to share the information without consent. This can be because it is overwhelmingly in the information subject's interests for this information to be disclosed. It is also possible that a public interest would justify disclosure of the information (or that sharing is required by a court order, other legal obligation or statutory exemption).

In the context of safeguarding a child or young person, where the child's welfare is paramount, it is possible that the common law duty of confidence can be over overcome. Practitioners must consider this on a case-by-case basis.