Ending domestic abuse

Sharing information to reduce the harm caused by domestic abuse

A Practitioner's Guide – Scotland

It is vital that any anxiety about sharing information does not stand in the way of protecting and promoting the welfare of adults and children living with domestic abuse.

Every practitioner must take responsibility for sharing the information they hold when necessary and appropriate to do so, and cannot assume that someone else will pass on information which may be critical to keeping someone safe.

Skilled practitioners are in the best position to use their professional judgement about when to share information, both within their own organisation, and with those working within other organisations, to provide effective early interventions, to improve their safety, and to keep families safe from harm. Lord Laming, chair of the Victoria Climbié enquiry in England, emphasised that it is always in the public interest to prioritise the safety and welfare of children.

GDPR and DP Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce 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, 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.

Further reading:
Guide to General Data Protection Regulations 2018
The DPA 2018

Summary

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. All organisations should have arrangements in place, which set out clearly the processes and the principles for sharing information.

Sharing Information is a fundamental part of a frontline practitioner's job. It is essential for accurate risk assessment to effectively protect adults and children from harm, and allows us to identify the needs for the whole family. 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 or risk from becoming more critical and difficult to address. It is a key factor identified in many domestic homicide reviews (DHRs) and serious case reviews (SCRs), that poor information sharing has resulted in missed opportunities to take action that keeps families and individuals safe.

Where there are concerns about the safety of a child or adult at risk, the sharing of information in a timely and effective manner between organisations, can improve decision-making. Information sharing is risk led; the greater the risk identified the more information can be shared (with or without consent, see below). It follows that information needs to be shared between agencies and practitioners so that they can analyse that information using their professional judgment to better understand and identify risks accurately.

We compare this process to a dimmer switch – the light becomes brighter the more you turn the switch until all becomes clear. Where it is personal and sensitive information (data) that is shared, turning that dimmer switch must be done thoughtfully, carefully and with a demonstrable lawful basis to increase the information shared. It may be that information is shared with one, two or three services before you are satisfied the risk is such that the information should be shared widely to ensure the best multi-agency response.

The Seven Golden Rules to Sharing Information

1. 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.

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, 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 principles

Article 5 of the GDPR sets out seven key principles which lie at the heart of the general data protection regime.

The principles lie at the heart of the GDPR. Compliance with the **spirit** of these key principles is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the requirements of the GDPR.

Article 5 paragraph (1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation')

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

(d) accurate and, where necessary, kept up to date; ('accuracy')

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; ('storage limitation')

(f) processed in a manner that ensures appropriate security of the personal data, ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

When should information be shared?

The most important considerations with respect to sharing of information are whether or not the proposed sharing of information would be:

1. likely to **support effective safeguarding** and promote the welfare of children; young people and adults who are at risk of harm;

2. likely to **aid accurate risk assessments**;

3. likely to **inform decisions about suitable services** that can be offered to reduce risk; promote the welfare and improve the lives for the whole family and the individuals within the family.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection those who may be at risk. **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 someone at increased risk of harm.

Practitioners should ensure that enough information is shared, as well as consider the urgency with which to share it.

Purpose

First, establish your purpose for sharing information. What do you hope to achieve by sharing the personal data of an individual? Domestic abuse and child and adult protection require a collaborative multi agency approach to be effective.

No single agency or individual can see the complete picture of the life of a family or individual within that family, but all may have insights that are crucial to their safety and wellbeing. A victim of abuse, adult or child, identified to be at high risk of serious harm or homicide requires a coordinated, multiagency response. This requires all agencies to share relevant information in order to develop an action plan that is comprehensive, robust and addresses the risk to and/or posed by all parties.

The purpose of sharing information is to accurately assess and address the risk and needs of families affected by domestic abuse. This means that information must be shared as soon as concerns are identified, before the risks increase and the needs become so complex that they become difficult to address.

Lawful basis for sharing information

All information must be shared lawfully, fairly and in a transparent manner. Sharing information is only lawful if you have a lawful basis under Article 6 of the GDPR. You must use personal information in a way that is fair. This means you must not share information in a way that is “unduly detrimental, unexpected or misleading to the individuals concerned”.

There are six options for lawful basis to share information and which one is relevant will depend on the **purpose** for which you are sharing. No single basis is ‘better’ or more important than the others, but at least one must apply. You must be clear, open and honest with people from the start about how you will use and share their personal information

You should make a decision as to which basis is more relevant, based upon each case, circumstance and with respect to local policy and protocols and you must determine this before you begin sharing and processing information. You should also document your decision.

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life (*please note that the risk to life needs to be immediate and therefore it is a less likely basis to be used in a multi-agency setting*).

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests

There are also specific additional conditions for processing especially sensitive types information; for more information, see our **Information Sharing Toolkit**. Your local Information Sharing Policy and Marac Operating Protocol should detail the purpose for sharing information and the lawful basis. The privacy notice should include your lawful basis for processing as well as the purposes of the processing.

A word about consent

GDPR sets a high standard for consent. But you *often* won't need consent. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your professional relationship.
If you have assessed a victim of domestic abuse to be at high risk of serious harm or homicide (i.e. meeting the Marac threshold) then you will have grounds for sharing information in law. This means that the individual does not have choice and is not in control of information sharing; however, you should still explain how and why you are sharing information.

Asking someone if they consent, implies that they can say no and that you will respect their wishes. In the circumstances outlined above, if you would still share personal information in order to protect them from harm, even if the person did not want you to, asking their consent is misleading, unfair and confusing. It is important that practitioners feel confident in giving clear and sensitive explanations to service users about their decision to share their personal information.

For transparency, we suggest you record your decision-making process at every stage.

Please note that requiring consent to share information is different from seeking consent to engage with a service, as this often can often get confused.

What information should be shared?

Practitioners should use their professional judgement when making decisions about what information to share and should follow organisational procedures and relevant policies or consult with their manager or information/data protection officer if in doubt. When recording and documenting information, it is essential that you distinguish between **fact** and **opinion**.

Necessary and proportionate

Not every bit of information held by practitioners needs to or should be shared. When making decisions about what information to share, you should consider how much information you need to provide. Not sharing more information than is necessary is a key element of the GDPR and Data Protection Act 2018. You should consider the impact of disclosing information on the person whom the information relates to and any third parties. Information must be proportionate to the need and level of risk. It is possible to lawfully share information regardless of risk level identified. Indeed, information sharing is necessary to make an accurate risk assessment.

Consider **who** needs to know the information to make an assessment of risk and needs and how much information is adequate for them to achieve that purpose. Your local Privacy Impact Assessments/Information sharing protocols should support you in your decision making.

Relevant

Only information that is relevant to the purpose 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 clearly stated.

Record

Every decision to share *or not* to share information should be recorded. If the decision is to share, justification 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.

How should information be retained and stored?

Secure

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

Retention

Each organisation will have a retention policy and, in line with this, the information should not be kept any longer than is necessary.

Very rarely this may be indefinitely. Instead, it may be for several years, and when this is the case there should be a review process scheduled at regular intervals to ensure information is not retained where it is unnecessary to do so and to ensure that the information retained is accurate and up to date.

Important

Local governance structures and information sharing protocols can help to ensure that a culture of appropriate information sharing is developed and supported as necessary through regular accessible multi-agency training.

This guidance is designed as a 'pocket guide' to empower practitioners and mangers to feel confident in why, when and how they share information. All advice and guidance reflects the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

We recommend that all practitioners have access to expert advice, information sharing policies and support within their organisations to share information with confidence.

The following documents partner or complement this simple guide and we encourage using this guide to refer to these where appropriate.

Information Sharing Guidance

Our **Community Platform** is a great place to network with other domestic abuse practitioners, share ideas and find out what other services around the UK are doing in relation to good practice, including compliance with GDPR.