Ending domestic abuse

Information Sharing
GDPR and Data Protection Act 2018
Scotland Toolkit

Since 25th May 2018 all agencies have needed to demonstrate that they are compliant with the **General Data Protection Regulations** (GDPR) and accompanying **Data Protection Act 2018** (DPA) and must have appropriate policies in place.

Whilst SafeLives cannot provide legal advice on this subject and recommend that you seek the advice of a qualified legal professional, we understand that information sharing legislation can appear complex and daunting. In this briefing, we aim to offer guidance around the safe sharing of information. We have included links to relevant areas of the **Information Commissioner's Office (ICO) Website** which we hope will ease navigation around their comprehensive guidance online.

In order that organisations, agencies and practitioners collaborate effectively, it is vital that everyone working with children and families, including those who work with parents/carers, understands the role they should play and the role of other practitioners. They should be aware of, and comply with, the published arrangements set out by the local child and adult protection plans. We recommend that all practitioners have a good working knowledge of Data Protection and that employers facilitate the development of this knowledge amongst their staff. We also recommend an understanding of child and adult protection legislation, as outlined within this guidance, and the **Information Sharing Toolkit Scotland** may be of interest. The **National Guidance on Child Protection in Scotland (2014)** highlights the need to share information about child protection concerns at an early stage.

Decision-making should be done in consultation with others within your organisation or with the Information Commissioner's Office Scotland: 0303 123 1115, scotland@ico.org.uk. Alternatively, legal advice should be sought where appropriate. It is the responsibility of each agency to ensure compliance in terms of what and how information is shared and stored. Whenever you are sharing personal data with other organisations, you need to be able to demonstrate you have carefully considered all aspects of data protection, and have established a clear lawful basis on which your decision to share information is based.

This toolkit can be used as a guide in situations where it may be necessary or desirable to share information with other agencies. Throughout we use specific information sharing terminology such as 'processing'. The ICO have produced a **glossary** that you may find useful.

Information about adults, children and young people at risk should only be shared between agencies:

- where relevant (there is a rational link to the purpose) and limited to what is necessary, not simply all the information held
- in a manner adequate and sufficient to properly fulfil your stated purpose for sharing information
- with the relevant people who need all or some of the information; and
- when there is a specific need for the information to be shared at that time.

Information so shared must only be retained for the minimum period possible, then securely destroyed.

Seven Principles of Data Protection

Article 5 of the GDPR sets out **seven key principles** which lie at the heart of general data protection. Article 5(1) requires that personal data shall be:

"(a) processed **lawfully, fairly and in a transparent** manner in relation to individuals ('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; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) **processed in a manner that ensures appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

(g) Article 5(2) adds that: Data controllers are responsible for and must be able to demonstrate compliance with Data Protection principles.

These principles lie at the heart of the GDPR. Compliance with the spirit of these key principles is a fundamental building block for good data protection and information sharing practice. It is also key to your compliance with the detailed provisions of the GPDR.

It is important to note that not complying with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines.

Lawful basis and legal grounds for sharing information

The first principle requires that you process all information lawfully, fairly and in a transparent manner. Sharing information is only lawful if you have a **lawful basis** under Article 6. And to comply with the accountability principle in Article 5(2), you must be able to demonstrate that a lawful basis applies. Note, that no basis is considered any 'better' than another.

The possible **lawful basis** are:

(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.

(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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

The individual's right to be informed under Article 13 and 14 requires you to provide victims/survivors of domestic abuse with information about your lawful basis for sharing. This means you need to include these details in your **privacy notice.**

You must use personal information in a way that is fair, meaning information should not be shared in a way that is "unduly detrimental, unexpected or misleading to the individuals concerned". In practice, this means being clear, open and honest from the start about how you use personal infomration.

We recommend that you have sight of your local relevant Privacy Impact Assessments or Information Sharing Policy and Operating Policy/Protocol, which will detail the purpose for sharing information and the lawful basis. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.

What is the lawful basis for sharing information in multi-agency working?

This depends on the purpose of that multi-agency process. In domestic abuse and child protection it is essential to share information:

- to assess risk and needs accurately,
- to intervene and provide the most effective and meaningful interventions

The lawful basis relied upon must be a decision made with consideration to the individuals and the circumstances at the time that the information is shared. As such, SafeLives cannot recommend a specific lawful basis or condition as it's important that the basis chosen reflects the nuances of the specific circumstance.

However, consideration could be given to the following lawful bases that are *likely* to be appropriate where it is necessary to share information for the purpose of assessing risk to adults and children living with domestic abuse.

Consent

GDPR sets a high standard for consent. You *often* won't need consent; consent means offering individuals **real choice and control**. Genuine consent should put individuals in charge, build trust, encourage 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 individual does **not** have choice and is not in control of information sharing through the Marac or child protection process. Consent to share information is different from consent to receive a service and this can often get confused.

Consent will not be the appropriate lawful ground for sharing information in the Marac process where the threshold of High Risk has been met. Nor will it be appropriate where a child is identified as being at risk of harm (s.26 Children & Young People (Scotland) Act, 2014).

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 that you record your decision making process. At all times, consider what information is **necessary** to be shared for the **purpose** you hope to achieve, what is **proportionate, relevant** and can you justify sharing that information?

Legal Obligation

The lawful basis for processing under legal obligation is almost identical to the old condition for processing in paragraph 3 of Schedule 2 of the 1998 Act. In short, when you are obliged to process the personal data to comply with the law.

Article 6(3) requires that the legal obligation must be laid down by UK or EU law. Recital 41 confirms that this does not have to be an explicit statutory obligation, as long as the application of the law is foreseeable to those individuals subject to it. So, it includes clear common law obligations.

This does not mean there must be a legal obligation requiring the specific processing activity. The point is that your overall purpose must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

You should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. For example, you can refer to a government website or to industry guidance that explains generally applicable legal obligations.

Grounds in UK and Scottish legislation which require or enable the sharing of information

Requirement	Legal authority
Prevention and detection of crime	s139 of the Antisocial behaviour (Scotland) Act 2004
To protect vital interests of the data subject; serious harm or matter of life or death	**Schedule 8, DPA 2018**
For the administration of justice (usually bringing perpetrators to justice)	**Part 3 & Schedule 8 DPA 2018**
For the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the protection against and the prevention of threats to public security.	**Part 3 s.31 & 35 DPA 2018**
Child protection. Disclosure to Children's Social Work or the Police for the exercise of functions under:	Children (Scotland) Act 1995, & Children & Young People (Scotland) Act 2014
In accordance with a court order	(requests to share information must show why it is relevant for the purpose for which they are requested, including a Court Order)
Overriding public interest	Common law
Right to life Right to be free from torture or inhuman or degrading treatment	**Human Rights Act, Articles 2 & 3**
Prevention of Abuse and Neglect	**Adult Support & Protection (Scotland) Act 2007**
Person lacks the mental capacity to make the decision regarding consent	**Adults with Incapacity (Scotland) Act 2000**

Legitimate Interest

Legitimate interest is the most flexible lawful basis, but you cannot assume it will always be appropriate for all your processing. Essentially, it is the equivalent Schedule 2 condition in the 1998 Act, with some changes in detail:

- The biggest change is the need to document decisions on legitimate interests to demonstrate compliance under the new GDPR accountability principle.
- You can now consider the legitimate interests of any third party, including wider benefits to society
- when weighing against the individual's interests, the focus is wider than the emphasis on 'unwarranted prejudice' to the individual in the 1998 Act
- GDPR is clear that you must give particular weight to protecting children's data.
- More information must be included in the privacy information provided

Public authorities are more limited in their ability to rely on legitimate interests and should consider the 'public task' basis instead for any processing they do to perform their tasks as a public authority.

Legitimate interests may still be available for other legitimate processing outside of those tasks. In practice, for instance, the police are the authority that upholds the law but in the Marac process it is necessary for them to share information to inform accurate risk assessments and this does not necessarily fit within their public task.

Relying on legitimate interest for data sharing can be broken down into a three-part test

Purpose test

Are you pursuing a legitimate interest?

Necessity test

Is the processing necessary for that purpose?

Balancing test

Do the individual's interests override the legitimate interest?

If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected.

Legitimate interest is most likely to be an appropriate basis where you use data in ways that people would reasonably expect and that have a minimal privacy impact. Where there is an impact on individuals, it may still apply if you can show there is an even more compelling benefit to the processing and the impact is justified.

You can consider legitimate interests for processing children's data, but you must take extra care to make sure their interests are protected. See the ICO's detailed guidance on **children and the GDPR**.

You may be able to rely on legitimate interests in order to lawfully disclose personal data to a third party.

You should consider

1. Why the organisation(s) with whom you are planning to share data with want the information
2. Whether they actually need it, and
3. What they will do with it.

You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

Public Task

The public task basis in Article 6(1)(e) is similar to the old condition for processing for functions of a public nature in Schedule 2 of the Data Protection Act 1998. "Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"
One key difference - GDPR says that the relevant task or function must have a clear basis in law.

You should **document** your lawful basis so that you can demonstrate that it applies. In particular, you should be able to identify a clear basis in either statute or common law for the relevant task, function or power for which you are using the personal information (accountability).

Update your privacy notice to include your lawful basis and **communicate this** to the client/service user.

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose. The focus should be on demonstrating either that you are carrying out a task in the public interest, or that you are exercising official authority.

Article 6(3) requires that the relevant task or authority must be laid down by domestic or EU law. This will most often be a statutory function. However, Recital 41 clarifies that this does not have to be an explicit statutory provision, as long as the application of the law is clear and foreseeable. This means that it includes clear common law tasks, functions or powers as well as those set out in statute or statutory guidance.

You do not need specific legal authority for the particular processing activity. The point is that your overall purpose must be to perform a public interest task or exercise official authority and that overall task or authority has a sufficiently clear basis in law.

Who can rely on this basis?
Any organisation exercising official authority or carrying out a specific task in the public interest. The focus is on the nature of the function, not the nature of the organisation.

Vital Interest

This basis is very similar to the old condition for processing in paragraph 4 of Schedule 2 of the 1998 Act. BUT: **anyone's vital interest** can now provide a basis for processing, not just those of the data subject. You are likely able to rely on vital interest if processing personal data is necessary to protect someone's life, however, you need to clearly demonstrate the immediate risk to their life. This means 'vital interest' is unlikely to be the most appropriate lawful basis for sharing information in a multiagency arrangement where other lawful bases may be more appropriate, less intrusive and easier to justify.

It is important to note that you cannot rely on vital interests for **health data** or **other special category data if the individual is capable of giving consent,** even if they refuse their consent BUT you can rely on other lawful bases (as above) without consent where the sharing of that information is necessary to achieve the purpose (e.g. to assess risk in Marac).

When is information sharing necessary?

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. Many of the lawful bases for sharing information depend on the processing being 'necessary'. This does not mean that sharing information always must be essential. However, it must be a **targeted and proportionate** way of achieving the **purpose**. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

Purpose

The purpose of sharing information in a coordinated community response to domestic abuse (and any associated process) is to protect adult and child victims of domestic abuse by assessing and responding to risk and need.

At the heart of a multi-agency collaborative response to domestic abuse is the working assumption that no single agency or person can see the complete picture of the life of an individual or family, but all may have insights that are crucial to the safety of that family and the individuals in it. To identify and assess risk and needs accurately, agencies need to share relevant information that is necessary and proportionate to fulfil this purpose.

The amount and depth of information shared will be informed by risk and the clearer the picture of risk, the more information can be shared. It follows therefore that information sharing is a dynamic process, where the greater the risks, the greater depth of information can be justifiably shared.

Special category and criminal conviction information

Special category data is data which GDPR says is more sensitive and therefore requires more protection. Examples include race, ethnic origin, religion, trade union membership, genetics and sexual orientation.

If you are sharing **special category data** you need to identify both a lawful basis for general processing under Article 6 and an additional condition for sharing this type of information under Article 9. These do not have to be linked. There are ten conditions for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and protections. The conditions are listed in Article 9(2) of the GDPR on the **ICO Website.**

In brief:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

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 employment and social security and 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 is carried out in the course of its legitimate activities

e) processing relates to personal data which are manifestly made public by the data subject

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity

g) processing is necessary for reasons of substantial public interest which shall be proportionate to the aim pursued, respect the essence of the right to data protection

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

i) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

If you are processing criminal conviction information or information about offences you need to identify both a lawful basis for general processing under Article 6 and an additional condition for processing this type of data under Article 10.

It makes sense that it is *necessary* to share information about an alleged offender/perpetrator of abuse with all agencies who are working to assess risk for the purpose of protecting victims and children. How much information is a decision to be made by individuals or agencies but it should be adequate to achieve the purpose. This may include details of convictions that are relevant – for instance, to demonstrate a propensity to violence; capability to break and enter; actions that may indicate the capability to kill or cause serious harm such as (but not limited to) strangulation; arson; harming pets/animals.

GDPR and data protection do not create a barrier to sharing this information, but they do demand greater consideration and accountability for sharing proportionate and relevant information, necessary to enable accurate risk assessment. Decisions should be recorded and clearly identified. Sharing information about a perpetrator of domestic abuse is essential to reduce the risk they pose to adult and child victims of domestic abuse identified at risk.

Children

Everyone has a responsibility for keeping children safe. No single practitioner can have a full picture of a child's needs and circumstances and, if children and families are to receive the right help at the right time, everyone who encounters them has a role to play in identifying concerns, sharing information and taking prompt action.

Practitioners working in Scotland should have a working knowledge of Child Protection Arrangements and corresponding legislation. The **National Guidance for Child Protection in Scotland (2014)** states:

"When gathering information about possible risks to a child, information should be sought from all relevant sources, including services that may be involved with other family members. Relevant historical information should also be taken into account"

Partnership working is also at the heart of GIRFEC (Getting it Right for Every Child, 2015):

"People working with children, young people and their families must work in partnership with them when considering and sharing information necessary to promote, support or safeguard a child or young person's wellbeing"

Children and Young People

GDPR explicitly states that children's personal information merits specific protection. GDPR contains provisions intended to enhance the protection of children's personal information and to ensure that children are spoken to in plain, clear, age appropriate language that they can understand. Transparency and accountability are important where children's information is concerned.

As with adults, you need to have a lawful basis for sharing a child's personal information and you need to decide what that basis is before you start sharing. You can use any of the lawful bases for processing set out in the GDPR when sharing children's information. But for some bases there are additional things you need to think about when your data subject is a child.

If you wish to rely upon legitimate interests as your lawful basis for processing, you must balance your own (or a third party's) legitimate interests in sharing information against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to protect against those risks. For more detailed guidance see the **ICO Website.**

Accuracy

You should take all reasonable steps to ensure the information you share and hold is not incorrect or misleading as to any matter of fact.

A record of an opinion is not necessarily inaccurate personal data just because the individual disagrees with it, or it is later proved to be wrong. Opinions are, by their very nature, subjective and not intended to record matters of fact. However, in order to be accurate, your records must make clear that it is an opinion and, where appropriate, whose opinion it is. If it becomes clear that an opinion was based on inaccurate data, you should also record this fact in order to ensure your records are not misleading.

Health

The current **NHS Scotland Information Sharing Guidance** states that only information may be shared with other organisations "to investigate or prevent a serious crime, or **to protect a child or vulnerable adult from harm**". "Any information shared will be appropriate, relevant and proportionate to the purpose of the sharing"

Caldicott Guardian Principles

Guidance has been published jointly by the Department of Health and the **UK Council of Caldicott Guardians** to assist those who need to share information about individuals involved in domestic abuse. Specifically designed for Marac but equally applies to other multi-agency meetings, it sets out the underlying ethical considerations between confidentiality and information sharing and identifies the role of the **Caldicott Guardian** to 'strike the balance' between maintaining the individuals' confidentiality and privacy and wider considerations such as protection from harm.

The report **'Striking the Balance': Practical Guidance on the application of Caldicott Guardian Principles to Domestic Violence and Maracs (Multi-agency Risk Assessment Conferences)'** provides context for sharing of health information sharing within Marac**.**

Subject Access Requests (SAR)

Individuals have the right to access their personal data that you hold. A subject access request can be made verbally or in writing. You have one month to respond to a request. The right of access, (referred to as subject access requests, or SAR), gives individuals the right to obtain a copy of their personal information as well as other supplementary information. It helps individuals to understand how and why you are using their information, and check you are doing it lawfully.

It is important to remember that Marac is not a legal entity. The information processed through the Marac process is the responsibility of the individual agencies and so any SAR for information shared at Marac must be addressed to the individual agencies who took the decision to share that information. This does not prevent an agreement being reached between agencies locally to enable the Marac administration agency to make decisions and disclosures of appropriate information. We recommend that any such arrangement receives appropriate legal scrutiny to satisfy all agencies who would be impacted in the event their information is disclosed in a SAR. The process for Maracs responding to an SAR should be outlined in your Marac Information Sharing Protocol (ISP).

An individual is only entitled to *their own* personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data. For further information about the definition of personal data please see the ICO guidance on **what is personal data**.

GDPR does not prevent an individual making a subject access request via a third party such as a solicitor. Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual (perhaps the perpetrator). The DPA 2018 says that you do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, you must consider all the relevant circumstances, including:

- the type of information that you would disclose;
- any duty of confidentiality you owe to the other individual;
- any steps you have taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

This means that although you may sometimes be able to disclose information relating to a third party, you need to decide **whether it is appropriate to do so** in each case. This decision will involve **balancing the data subject's right of access against the other individual's rights**. If the other person consents to you disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway. It is important to note that **valid consent must be freely given** and in cases of domestic abuse, it is vital to be alert to victims being coerced into 'consenting'.

Under the Data Protection Act 2018 (DPA 2018), it is an offence to make any amendment with the intention of preventing its disclosure.

For more information about Subject Access Requests please see the **ICO website**

Balancing principles: Rights of the individual

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

See the **ICO Guide** for more information.

Record all decisions and reasoning for decision making whether that decision is to share information or not to share information.

Balancing considerations

Proportionate response

- Respective risks to and safety of those affected
- Relevancy & proportionality
- Pressing need
- Need to know of other agencies (e.g. to inform risk/needs assessment)
- Sharing is necessary for the purpose
- Sharing information is justifiable
- The rights of the individual

Article 5 (1)(c) says:

1. Personal data shall be:
   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)

We recommend that all practitioners and agencies keep a data sharing log which demonstrates what information is being shared, why and with whom. It should include your decision making and thought process. Having this on file will demonstrate compliance with DP and GDPR and reflect high standards of good practice. Below you will find a suggested template that could be adopted and adapted for your agency's use.

Data (Information) Sharing Log

You are accountable for the decisions made regarding information sharing. Your decisions on sharing information must be justifiable and proportionate, based on the potential or actual harm to adults or children at risk and the rationale for decision-making should always be recorded.

Confidentiality must not be confused with secrecy. Decisions to share or not to share information, should be made with consideration of the safety and wellbeing of affected parties at the heart of those decisions. **If in doubt, always seek specialist advice and always consult with your supervisor or line manager.**

Data Subject (Client) Number	**Practitioner's Name:** **Please note here the name of anyone involved in decision making including manager or data officer**
Purpose *(What do I want to achieve by sharing this information? e.g. to enable effective risk assessment)*	**Lawful Basis** *(Make reference to condition/s & any relevant legislation and/or local protocol relied upon)*
Transparency *Has the data subject been told their personal information will be shared/have they seen a Privacy Notice? (note date, time and reasons for NOT informing them if that is the case)*	**Balancing exercise** *Has consideration of the interest of the other agency/person in receiving the information been given? And the degree of risk posed to any person by disclosure/non-disclosure. Consider the duty of interest. Record this. Record whether the sharing is proportionate, that there is a pressing need and summarise why*
What information is being shared *(be clear)* **and with whom** *What is the amount of information to be disclosed and the number of people/agencies disclosed to? Is this no more than strictly necessary to meet the purpose for disclosure? Record why this is the case.* *The information must be necessary and adequate to achieve the purpose noted above. It must be relevant and proportionate*	**What information that may be relevant to the purpose are you NOT sharing?** *Giving reasons for not doing so*