MULTI-AGENCY DOMESTIC VIOLENCE INFORMATION SHARING PROTOCOL GUIDANCE

This document focuses specifically on information sharing in relation to domestic violence. It is not intended to be a comprehensive guide to information-sharing in other contexts.

Background and rationale

• What is the purpose of a multi-agency information sharing protocol?

Research and experience have repeatedly shown that providing survivors of domestic violence and their child(ren) with effective protection from harm, requires professionals to share information about:

• a survivor who may need help
• a non-abusing parent who may need help in caring for their children
• anyone that may pose a risk of harm to others including child(ren) (for example perpetrators of domestic violence).
• a child's health, development and exposure to possible harm.¹

A multi-agency information sharing protocol highlights the roles and responsibilities of each partner agency and what information they will share and with whom they will share it with. Protocols should enable workers and agencies to share concerns about safety and to develop strategies to manage risk.²

Who is this guidance for?

This guidance is for those seeking to develop a multi-agency information-sharing protocol. It aims to inform professional decision-making to share personal information with partnership agencies to protect victims and enable perpetrators to be held accountable for their behaviour.

Effective multi-agency working is crucial to the aim of prioritising the safety of the abused woman and her child(ren). Whilst acknowledging that each agency maintains independence, it is important to ensure that all agencies who are signatories to the protocol have agreed to work in an integrated and co-ordinated way.

² Direct quotation from Respect’s Statement of Principles and Minimum Standards of Practice for Domestic Violence Perpetrator Programmes and Associated Women’s Services (May 2004).
Structure / suggested component parts of a multi-agency information sharing protocol

Statement of intent

This sets out the purpose and aims of the protocol.

The principle aim of an information sharing protocol should be to prioritise the safety of the abused woman and her child(ren).

If the right information is shared responsibly it can significantly enhance women and children’s safety.³

The intention is that a single, joint approach to exchanging relevant information which protects and enhances safety, is implemented as one of a range of mechanisms for reducing domestic violence.⁴

Wherever possible, steps must be taken to hold the perpetrator accountable for the abuse. Practitioners must not place the onus upon the survivor to do this. The stage at which the perpetrator is ‘within the system’ should be identified using manual and electronic tracking to identify risk.⁵

Additional aims of multi-agency information sharing protocols should be:

- to identify any problems or difficulties with the services being provided to the survivor and their child(ren).
- to collate all the information on each case and also to record the point at which a case is referred to other agencies.
- to enable agencies to deliver effective services.
- for monitoring and accountability purposes. To ensure that agencies involved are adhering to their protocols and procedures.
- to avoid duplication of effort (e.g. record taking, service provision)
- for agencies to feel confident that they can provide a comprehensive, safe, quality service to clients, within the provisions of the law.
- for agencies to enhance their reputation for professionalism and credibility with clients and other agencies by demonstrating their competence.⁶

³ Ibid.
⁴ Adapted from Information Sharing Protocol Domestic Abuse MARAC (Multi-Agency Risk Assessment Conference).
⁵ Adapted from Woman’s Trust Advocacy Service Protocol on data sharing (October 2004).
⁶ Adapted from Safety and Justice: sharing personal information in the context of domestic violence - an overview Home Office Development and Practice Report 30.
http://www.homeoffice.gov.uk/rds/pdfs04/dpr30.pdf
What the protocol should do for victims/survivors and their child(ren)

Responsible multi-agency information sharing enables:

- timely action to protect clients and children from further abuse
- comprehensive risk identification and safety planning based on a full account of the facts and circumstances of each client’s situation
- the right sort and combination of advice, support and advocacy to be offered at the right time based on a full and accurate account of the client’s needs and history, including other service contact and use.
- clients to avoid the added distress of having to repeat details of their history and experience of domestic violence each time they access a different service
- agencies to work together to protect victims of domestic violence and their children in an informed and comprehensive way.  

Agreed definition of domestic violence

Multi-agency protocols must have agreed definitions if they are to work. To avoid unnecessary duplication of effort we would recommend that the Government’s definition be used. This definition is:

‘Any incident of threatening behaviour, violence or abuse (psychological, physical, sexual, financial or emotional) between adults who are or have been intimate partners or family members, regardless of gender or sexuality.’

This includes violence such as female genital mutilation (FGM), so called ‘honour’ crimes, forced marriage and acts of gender based violence.

Abuse of children is excluded from this definition of domestic violence. Nonetheless, research has shown that domestic violence and child abuse frequently co-exist. Research shows there is a correlation at least half of the time. Child abuse is dealt with via separate policies and procedures which since January 2004 include “impairment suffered from seeing or hearing the ill-treatment of another” i.e. living with domestic violence.

Commitment and engagement of all agencies

Signatories to a multi-agency information sharing protocol must recognise the importance of sharing information appropriately in order to maximise the safety of the survivor and her child(ren), and undertake to cooperate fully with each other within the parameters of legislation (see Appendix1) and with Government guidance associated with these Acts.

---


8 This section of the Adoption and Children Act 2002 amends the Children Act 1989, which came into force on 31 January 2005.
It is essential that there is the appropriate level of support at a management level in order to enable information sharing to take place effectively.

All agencies must pledge to consult regularly with each other upon matters of policy and strategy.

Each partner must recognise that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller: a person within the partner agency who determines both the purposes for which, and the manner in which, personal data is processed.

The agency receiving data will not share it with any other party without the disclosing agency’s permission.

Each party pledges to ensure that it is appropriately registered with the Office of the Information Commissioner for the purpose of sharing and receiving personal information for the purpose of crime reduction.

All agencies agree to seek their own legal advice, wherever necessary.\(^9\)

Chief Officers of each agency should formally agree to the following:\(^10\)

- to subscribe to the principles contained in the information sharing protocol;
- to work to the procedures identified within the protocol;
- to fully implement the protocol within their own agency, ensuring that all staff know of its existence to prioritise the safety of survivors of domestic violence and their child(ren), and to support their attendance at any training event required;
- to supply information within the bounds of the information sharing protocol at no financial cost to any of the other signatory agencies;
- to contribute to the development of trust and confidence between the signatory agencies by working within the framework of the information sharing protocol to disclose, retain and dispose of data for the purpose of supporting the aim of increasing the safety of a survivor of domestic violence and their child(ren).

**Accuracy**

Information held must be accurate and kept up to date. Steps must be taken to validate information, such as checking with the person who originally provided the information, if staff are in doubt as to its accuracy.\(^11\)

---

\(^9\) Direct quotation from Section 1.2 Commitment - Home Office Prolific and other priority offenders: information sharing protocol.

\(^10\) Direct quotation from section 8 Home Office Prolific and other priority offenders: information sharing protocol.

Individuals will be given the opportunity to inform staff if their circumstances change.

If the individual has informed the organisation that, in their view, the information is inaccurate, then a record should be made on the file that they have expressed this view.¹²

**Risk**

To establish the level of risk posed it will be necessary to exchange information on a range of individuals and this information may be stored where there is a justification to do so.¹³

Agencies and their employees are therefore expected:

- to take seriously concerns (informally or formally raised, anonymous or otherwise) regarding individuals who may threaten others in the community.
- to keep an open mind which does not pre-judge the situation.
- to investigate risks in an effective manner.
- to share information as specified in the multi-agency information sharing protocol.
- to offer best possible protection to the victim, the individual giving cause for concern, and the community. This means keeping a balance between acting responsibly in relation to the individual who presents the risk, on the one hand, and protecting the public from harm and maintaining safety in the community on the other.¹⁴

Any signatory agency may approach other signatory agencies for information if they have concerns about the risk of harm to the public or individual.

**Confidentiality and consent**

- Confidentiality in relation to the survivor

Agencies should ensure that perpetrators are never told whether their (ex) partner has had any contact with a service and in particular that no information on the nature or content of any contact is divulged.¹⁵

Agencies should explain to women:

- about their (ex)partner’s limited confidentiality and what information they may or may not have access to

---

¹² Ibid. P 6.
¹⁵ Adapted from Respect’s *Statement of Principles and Minimum Standards of Practice for Domestic Violence Programmes and Associated Women’s Services* (May 2004).
• about their own confidentiality  
• about the agency’s child protection policy  
• how information is shared between workers at different organisations and within the organisation.

Case workers have a duty to consult with their supervisor and / or Line Manager, where they have concerns and are unclear of how to proceed, so as not to increase the risk to the survivor or others.\(^{16}\)

Practitioners must be aware of how a breach of confidentiality and the revelation of the identity of a domestic violence survivor can impact on their safety. Requests from ‘professionals’ may actually be made by a perpetrator or by someone acting on behalf of a perpetrator. There are professionals who concede to bribes and break their code of ethics and information sharing policies and protocols.\(^{17}\)

• Cases which involve children and how to handle child protection issues

It is recognised that supporting the non-abusive parent is likely to be the most effective way of promoting and safeguarding the child’s welfare. However, the paramountcy principle enshrined in legislation means that the concern must be to safeguard the child whether consent has been given or not.\(^{18}\)

If there is reason to believe that a child has suffered or is likely to suffer significant harm, the agency must initiate child protection proceedings and contact the appropriate Social Services Child and Families Team who will make enquiries under Section 47 of the Children Act 1989.

In all other circumstances where there is concern that a child is at risk of harm, a referral should be made to Social Services (under Section 17 of the Children Act 1989 - children in need) who will ask other agencies to contribute to an initial assessment if one is to be undertaken.

Agencies that have had contact with the non-abusive partner should wherever possible give information about the role that they play in the child’s life and make recommendations that the relationship between non-abusive parent and child is not disrupted unduly by care proceedings.

• Young people

Where consent is needed to share information about a young person (under the age of eighteen), it should be sought from the non abusive parent who has Parental Responsibility

\(^{16}\) Adapted from Para 4.3 of Respect’s Statement of Principles and Minimum Standards for Domestic Violence Perpetrator Programmes and Associated Women’s Services (May 2004).
\(^{17}\) Directly quoted from Haringey Information Sharing Protocol.
(Section 2 (7) of the Children’s Act 1989). Consent can be gained from only one person with Parental Responsibility, rather than both parents.

A young person (below the age of sixteen) can give consent in their own right if it can be demonstrated that they are of sufficient age and understanding to understand the implications and consequences.

Agencies should also note that they also owe a duty of confidentiality to a young person in the same circumstances that they would do for an adult.\(^1^9\)

- **Confidentiality in relation to the perpetrator**

Information will only be used for the purpose for which it was requested, and will be securely stored and destroyed when it is no longer required.

**Cautions and convictions**

The prevention of crime and administration of justice, as provided for in the Crime and Disorder Act 1998, are obviously in the public interest and may provide grounds upon which a disclosure of cautions and criminal convictions can be justified.

Details of convictions recorded on the Police National Computer, or retained on file by signatory agencies, can be released to a professional from another agency where this is justified in the public interest, to support proceedings under the Crime and Disorder Act 1998. Great care must be taken to ensure conviction data is accurate, up to date and relevant to an enquiry before it is released.

**Personal data shared with consent\(^2^0\)**

Personalised information should only be shared for the purpose of increasing the safety of the domestic violence survivor and their child(ren).

It is the responsibility of each agency to seek the consent of the survivor where it is needed to obtain personal information. There should be a section on a domestic violence information sharing form for the domestic violence survivor to give their written consent for each piece of information that is requested, thus ensuring that a general consent is not given and the domestic violence survivor consents fully each time different information is asked for from another agency. Obtaining explicit consent from the survivor is good practice and should be sought from and freely given by the data subject.\(^2^1\)

---

\(^1^9\) Directly quoted from Warwickshire Crime and Disorder Protocol (October 2002) p.5.

\(^2^0\) This section is adapted from section 3. Home Office *Prolific and other priority offenders: information sharing protocol*.

\(^2^1\) Adapted from Haringey Information Sharing Protocol.
It is imperative that survivors are made aware of all the implications for sharing sensitive information. The Home Office has issued guidelines for this procedure and has provided the following checklist for practitioners:

<table>
<thead>
<tr>
<th>A checklist for practitioners</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Has the client been informed of the reasons why her data may be shared?</td>
</tr>
<tr>
<td>• Has the client been informed of what information may be shared, when and with whom?</td>
</tr>
<tr>
<td>• Has the client been reasonably informed of the implications of her granting consent?</td>
</tr>
<tr>
<td>• Has the client been informed of her right to refuse consent, give partial consent (i.e. allow the sharing of some information) or withdraw it at any time?</td>
</tr>
<tr>
<td>• Have measures been put in place to ensure that the client will be kept-up-to-date with the information sharing process in relation to her information?</td>
</tr>
</tbody>
</table>

Appropriate translation services need to be provided if the survivor is unable to communicate in English. Other communication issues for example, being deaf or having low literacy levels will also need to be taken into consideration and provision made for the client. Agencies must find a way of ensuring the client is able to communicate and this is a key part of providing a client-centred and culturally sensitive service.²²

Each client’s needs should be assessed on an individual basis and additional steps taken such as the publication of information in a range of languages, use of translators, and/or involvements of advocates to ensure that clients can give informed explicit consent.²³

**Gaining explicit verbal consent**

In contexts where obtaining written consent is impracticable (eg. telephone advice services) documented verbal consent can be obtained.

Monitoring forms should be used to record client details and clients asked if they are willing for their details to be passed to relevant partner agencies.

Where verbal consent is sought, the procedure should be evidenced and it is recommended that:

• a standard form of wording is used to request consent that covers the requirements of ‘explicit consent’;
• the time, date and identity of the person seeking the consent are recorded;

---

²² Ibid.
• the decision of the client is recorded; (eg ‘Consent Given’. ‘Consent Denied’. ‘Consent Not Sought’. Any other advice or action taken should also be recorded);
• relevant action such as any disclosure of information taken following the granting of consent is recorded.

In most cases, consent can be sought when clients first come into contact with an organisation. However, many frontline service providers encounter clients when they are emotionally distraught, disorientated and/or physically injured and it may not be possible to obtain explicit consent to share information at this time. Professional judgement will come into play in making an assessment as to when would be a good time to seek consent.

Timely decision-making about sharing information is often crucial to protecting victims.

It should not be assumed that consent of the survivor is always necessary in order for agencies to share information although consent of the survivor must be sought and should ideally be obtained before disclosing information.

However, in the case of perpetrators the aims of increasing safety of the survivor and their child(ren) might be prejudiced if agencies were to seek their consent. In such cases the disclosing agency must consider possible grounds to override the consent issue.

It is possible to disclose personal information without consent if this is in the defined category of public interest.

Sharing information without consent

A consent based approach to the sharing of information is good practice. However under the Data Protection Act, consent is only one of the schedule 2 and 3 conditions that will allow personal and sensitive data to be processed. Sadly, there will be situations and circumstances where there is a need to share information without consent in order to protect the victim and/or child(ren), share information with specific agencies for risk assessment purposes or to bring perpetrators to justice.

Practitioners will need to make a careful assessment and consult with their line manager at the outset of their decision-making as to whether they should set aside the consent-based approach. This is because if consent is sought but then refused, it is not good practice to share data on a different basis. If circumstances are such that there is a justifiable and pressing need to share information in serious and justifiable circumstances that do not require a consent based approach, it is advisable to pursue this from the outset, informing the victim about the information-sharing.

Three contexts covered by the Data Protection Act where consent is not required:

• *Where ‘vital interests’ of the client are at risk.*
This is where information sharing is necessary for matters of life and death or for the prevention of serious harm to the individual.

- **Where processing is necessary for the purposes of ‘administration of justice’**

This condition can apply to processing data about victims or perpetrators of domestic violence. However, as consent may not be forthcoming from perpetrators, the ‘administration of justice’ provisions may be particularly applicable when processing data to try to bring them to justice.

- **Where processing is for public/statutory functions**

The Data Protection Act makes provision for processing which is necessary in the ‘public interest’.

**Withdrawal of consent**

The service user is entitled to withdraw their consent to the sharing of information at any point during assessment or provision of services.

The service user must be informed that she or he can exercise this right and that, should they do so, they will be informed of any potential impact on service delivery.

In the event that an individual:

- withdraws her/his consent for their personal information to be shared,
- wishes to subsequently place / amend restriction upon the personal information to be shared

the agency receiving such a request will immediately inform all other agencies who are, or may be, affected and record the details on the individual’s file.

In the case of consent being withdrawn, no further personal information should be disclosed unless there are statutory reasons for doing so, or legal exemptions can be applied (as detailed above).

---

24 This section is adapted from Barnet Safe sharing of Information - for Social Services. Rachel Smith (2006).
No duress

The procedures for obtaining consent will recognise the need to handle consent seeking in a sensitive manner.

It will be fully explained to the individual what they are being asked to consent to and care will be taken to ensure they have understood this.

Any member of staff who may have to seek the consent of a person to share information about them, will be trained to present and explain the issues to the individual in a positive and sensitive manner. Consent seeking will only be carried out by staff who have been trained in procedures.

Individuals can object to agencies sharing their personal data on the following grounds:

• the right to prevent processing which is likely to cause them damage or distress
• the right to prevent processing for purposes of direct marketing
• the rights to not allow automated decision making in relation to them
• the right to compensation via the courts if the Data Protection Act 1998 is contravened

An individual is entitled to serve upon an organisation a written notice requiring them to cease or not begin processing their information, where such processing is causing or is likely to cause unwarranted substantial damage or substantial distress to them or to someone else.

However, this right is unavailable in certain circumstances including where:

• the data subject has given their consent to the processing
• the processing is necessary in order to protect the vital interests of the data subject.

It is important to note, however, that the factor of public interest can override these grounds.

---

26 This section is quoted from A general framework for information sharing in social services Department of Health August 2003.
27 An individual is entitled, by written notice, to require an organisation to ensure that no decision which significantly affects them is based solely on the automatic (i.e. no human intervention in the) processing of information. Ibid.
28 Individuals have the right to seek compensation via the courts if they suffer damage or distress as a result of any contravention of the requirements of the Data Protection Act if the organisation cannot prove that they have taken reasonable care in the circumstances to comply with the Data Protection Act. Ibid.
29 This section is adapted from section 3. Home Office Prolific and other priority offenders: information sharing protocol.
Requests for assessment\textsuperscript{30}

An individual, may ask the Data Protection Commissioner to assess whether or not it is likely that any processing of information has been or is carried out in compliance with the Act. This may lead to enforcement action if it is pursuant to a complaint against the organisation.

\textbf{Data}\textsuperscript{31}

There are three types of data: non-personal, depersonalised and personal data. The sharing of non-personal and de-personal data in domestic violence cases is not generally problematic.

\textbf{Non-personal data}

Signatory agencies must understand that non-personal data is data that does not, nor has ever, referred to individuals. It will often aggregate data derived from personal, non-personal data for crime-mapping purposes, within the remit of the Crime and Disorder Act 1998.

Signatories understand that non-personal data held may be subject to the provisions of the Freedom of Information Act 2000, and there may be a duty to disclose this data to a third party if a request is made under the Act.

\textbf{De-personalised data}

Depersonalised data encompasses any information that does not and cannot be used to establish the identity of a living person, having had all identifiers removed. Signatories recognise that great care must be taken when depersonalising data and that the Information Commission has stated that even a postcode or address can reveal the identity of an individual. Signatories should also be aware that it may be possible for an individual’s identity to be revealed by comparing several sets of depersonalised data.

Signatories must accept that there are no legal restrictions on the exchange of depersonalised data, although a duty of confidence may apply in certain circumstances which may prevent the information being disclosed to partners. This is to be decided on a case by case basis by the disclosing agency.

\textbf{Personal data}

Personal data is information which relates to a living individual who can be identified from that data.

\textsuperscript{30} ibid
\textsuperscript{31} This section is quoted directly from Home Office Prolific and other priority offenders: information sharing protocol
Women and child(ren)’s safety can depend on personal records being kept secure. Personal data should be clearly marked. Signatory agencies should undertake to destroy all personal data when no longer required for the purpose for which it was provided.  

Personal data must be stored securely. This is especially important if the abuser also accesses the service as a client, as notes may not only be accessed by a perpetrator but someone known to him who works for the organisation.

Any record of domestic violence should be kept separately from notes held by the client to which the abuser may have access (for example, medical notes). This includes their address if living separately from the abuser, or any other information that could place a woman and/or her child(ren) in danger.

All grounds for the disclosure of personal information under a multi-agency information sharing protocol will be formally recorded, and partners will process information fairly and objectively in every case.

Agencies agree to only disclose sufficient information to enable partners to carry out the relevant purpose for which the data is required. This will be determined on a case by case basis, through negotiation between disclosing and receiving partners where necessary.

Professionals may be concerned about recording information that could unintentionally harm a victim of domestic violence. All staff must be honest about their efforts to maintain confidentiality, and specific about the limitations. Professionals may be concerned about records later being used in court or by external agencies. It is important to acknowledge this. In many cases the survivor can submit a professional’s information without any direct contact between that professional and the agent requesting evidence.

Encouraging survivors to keep a diary and record the abusive incidents (but only if it can be done safely, in a hiding place or at a safe address) might also help in the long term. Whenever it is safe, agencies should encourage them to make careful notes of everything that happened, including times, dates, names, and what everyone said.

**Personal data collection systems**

Data collection systems or record-keeping do not need to be complicated or costly. It assists an agency or agencies in considering what service users need, and can help to make a case for improved funding and other resources.

32. This section is quoted directly from section 2.3 personal data. Ibid.
34. This section is quoted directly from section 2.3 personal data. Home Office Prolific and other priority offenders: information sharing protocol.
35. BMA 1998 quoted from Roxane Agnew-Davies and Jenny Phaure DVT Ltd Training for day 3 Kingston Training.
36. Ibid.
Secure storage of personal data

Personal information shared with other organisations will be extracted from internal systems by an organisation’s own members or staff in accordance with their own internal access and security arrangements.

Agencies will ensure that all personal files and confidential information are kept in secure, controlled locations when unattended e.g. in locked storage cabinets, appropriate protection for computer systems, laptops etc. Keys to locked storage should be held only by staff that need regular access to the information. Staff should only have access to personal information on a “need to know” basis in order to perform their duties.

Agencies should take every precaution to ensure that information identifying individual service users is transferred and shared in a secure manner. Agencies should also agree to conduct six monthly audits of security arrangements, to ensure they are effective.38

Procedures for transfer of information are given below.

Transfer of personal data between agencies

Electronic transfer of personal data
Transfer of personal information by email should be avoided unless the information is encrypted i.e. transmitted in a coded format. (This is because of concerns about the insecurity of the system. Security can be safeguarded through encryption). Multi-agency partners who want to use email for the transfer of personal information will need to agree between themselves a suitable form of encryption.

Instead of using email information can be transferred using a password-protected disc / electronic storage device.

If email is used (suitably encrypted) then an audit trail must be in place to track its’ usage. This should include details about the person using the system, the physical device from which they have accessed system and the functions they have carried out on the system and when they were carried out. Systems also need to be put in place for the monitoring and review of audit trails.

Transfer of personal data by fax
Personal information should not be transferred by fax, wherever possible. If it is necessary to use a fax because of a need for urgency then the following precautions should be taken.

Minimise the amount of information included in the fax. A “two fax” approach can be useful where personal details without identification details are sent on one fax, with the identifier

38 As recommended in MARAC Information Sharing Protocol.
sent on a separate fax. If the first fax went astray for any reason the second should not be sent.

Send information to a “Safe Haven” fax. A Safe Haven fax is one that is managed in such a way that its security is enhanced. These safeguards should include that:

- the fax is sited in a secure room or cupboard
- the recipient organisation has a written policy for handling faxes which staff have been informed about and understand
- identified staff are responsible for waiting by the machine until the fax is sent and for collecting and delivering faxed information to the appropriate person.

Telephone the recipient to ensure they are aware a confidential fax is about to be sent and confirm that an identified individual will collect and deliver it and that safe receipt will be confirmed.

Ensure that the fax is sent with a cover sheet stating that it is strictly confidential. The cover sheet should also state that the fax is for the intended recipient only and in the event of error the sender should be notified immediately.

There are some types of personal information which should never be transmitted by fax. These include details relating to HIV status, sexual health matters, drug use, mental health issues or incriminating evidence.

A log should be kept of confidential faxes sent, giving details of the sender and recipient, date and time of transmission and a copy of the printout form the fax confirming transmission success.

**Transfer of information verbally**

A considerable amount of information sharing takes place verbally, often on an informal basis. Difficulties can arise because of this informality particularly in open plan locations. Care should be taken to ensure confidentiality is maintained in such discussions.

If information is to be shared by phone, then steps need to be taken to ensure the recipient is properly identified. This can be done by taking the relevant phone number, double-checking that it is the correct number for the relevant individual / organisation and then calling the recipient back.

Where information is transferred by phone, or face to face, care should be taken to ensure that personal details are not overheard by other staff who do not have a “need to know”. Such discussions should take place in private locations and not in public areas, for example, reception areas. If this is not possible then, with the exception of emergencies, transfers of information should be carried out by more secure means.
Transfer of information by post

Written communications containing personal information should be transferred in a sealed envelope and addressed by name to the designated person within each organisation. They should be clearly marked “Personal and Confidential - to be opened by the recipient only”.

The designated person should be informed that the information has been sent and should make arrangements within their own organisation to ensure that the envelope is delivered to them unopened and that it is received within the expected timescale.

If an organisation has a policy that all mail is to be opened at a central point this policy must be made clear to all partner agencies. An alternative means of transfer should be arranged where it is essential that the information is restricted to only those who have a need to know.

The personal information contained in written transfers should be limited to those details necessary in order for the recipient to carry out their role.39

Data Controller and responsibilities40

For the purposes of this document the term Data Controller has been used. Agencies may already employ staff who fulfil a similar role but have a different job title, for example, Tracker.

Specific responsibilities will be:

- ensuring their agency abides by the agreed multi-agency information sharing protocol;
- ensuring that all Designated Officers and other staff are fully aware of their responsibilities;
- appointing other staff to act as Designated Officers in their absence;
- authorising their agency’s involvement and co-operation in the information sharing process, at every stage;
- keeping a protocol co-ordination folder, which holds all information sharing documents;
- ensuring their agency’s Data Protection Notification entry is accurate, up to date and adequate for the purpose for which it is intended.

Designated Officers are responsible for ensuring that processing of personal data is in accordance with the principles of the Data Protection Act (as stated previously).

Designated Officers are the data owners for each signatory agency. Only they can make formal requests and document agreements for the sharing of personal information under the information sharing protocol. They will also decide on a case by case basis when disclosure is necessary and when the public interest overrides the presumption of confidentiality.

39 This section is quoted directly from Sharing information: Leeds Inter-agency Protocol for Sharing Information - Operational Procedures (October 2002).
40 Directly quoted from section 4 Data Controller and responsibilities. Ibid.
They must also ensure ease of administration, covering all aspects and documentation of the information sharing process. This may be achieved by creation of a project or file, which must be kept up to date and include:

- record of data disclosed
- chronology of case
- information sharing access list
- notes of meetings with partners
- recent correspondence (including email) and phone calls.

The Designated Officer must also ensure that the information held is reviewed with partners regularly.

### An information sharing protocol should also include:

- a list of partners who have signed up to the protocol to share information with one another (appendix and update regularly).
- an equalities statement
- a statement on dissemination / circulation of the protocol. For example that the protocol will be introduced to managers and staff (employees, agency staff and volunteers) through a programme of multi-agency briefings and training events which will take place at least one month before any protocol becomes effective.
- detail on how the information sharing protocol will be reviewed. Information sharing protocols should be reviewed and updated on a regular basis.
- detail on the destruction and retention period of data. Signatories to an information sharing protocol must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice. An overarching principle of agencies should be to increase and protect the safety of the survivor and her child(ren). Partners must agree a maximum retention period for data.
- detail on publication of the protocol. The agreed information sharing protocol should be published and made available to the general public for clarity of purpose. Protocols should be published on the websites of the organisations involved and made available to service users.

---

41 Adapted from section 5 Ibid.
42 Directly quoted from section 5.4 Ibid.
• a statement on liaising with the media in relation to personal data. Signatories agree when liaising with the media to ensure there is a consistent approach to media enquiries and that staff do not express personal views and respect the requirement for confidentiality and discretion. Partner agencies should agree:
  - when providing information to the public, to do so honestly and fairly
  - statements should reflect the multi-agency decision making process;
  - consent of the data owner will be sought and obtained prior to release to the media.
  - all agencies undertake at all times to comply with data protection law and other legal requirements relating to confidentiality.

• detail on how the rights of ‘data subjects’ will be upheld including access to information, corrections and amendments or complaints. Suggested steps of a complaints procedure would be:
  - initial complaints being referred to the relevant Designated Officer
  - an agreement that any formal complaint by a data subject regarding any stage of the process will be notified (as a best practice measure) in writing to all partners
  - an agreement to undertake to do all possible within the guidelines of the Data Protection Act 1998, to assist with any complaint.
  - a recognition that individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman.

• a commitment to ensure that the training needs and peer support needs of staff will be met to enable them to effectively implement the information sharing protocol.

• steps to be taken following a breach of the information sharing protocol. Such as:
  - an agreement that any breach of confidentiality will seriously undermine and affect the credibility of crime audit work, partnership objectives, and render liable for breach of the law.
  - to undertake, at all times, to comply with data protection and other legal requirements relating to confidentiality.
  - and that any disclosure of information by an employee which is done in bad faith or for motives of personal gain will be the subject of an inquiry and be treated as a serious matter. Each party will be held accountable.

• an indemnity clause. As protocols are not legally binding documents, it is wrong to assume that mention of these indemnity clauses in any protocol would place all signatories beyond legal challenge, following a breach of disclosure of certain sensitive

---

43 Adapted from section 5.5 Media handling. Ibid.
information. It may be an option therefore to include an indemnity clause when developing a multi-agency partnership protocol.\textsuperscript{44}

In addition to this partnerships should develop:

- consent and information forms and leaflets for service users
- information or data sets for staff
- a definition of ‘need to know’ for staff
- an implementation plan for the multi-agency information sharing protocol.

Where can I find more information about information sharing protocols?

  Information line: 01625 545 745
- Home Office Information-sharing helpline: 020 7273 4015

\textsuperscript{44} Adapted from “Model” Protocol section on Crime Reduction website http://www.crimereduction.gov.uk/infosharing.doc
APPENDIX 1
Legislation and guidance

An overview for the legal basis of the protocol

Organisations have an obligation to act within the current legal framework with regard to information sharing and data protection.

Key legal instruments which form the basis for an information sharing protocol are:


- **Crime and Disorder Act 1998.** Section 115 which enables any person to disclose information for any purposes of any provision under the Crime and Disorder Act 1998 to a relevant authority, or to a person acting on behalf of such an authority. Sharing information to prevent the physical assaults, harassment and criminal damage that often constitute domestic violence would be in keeping with the purposes of the Act.

- **Domestic Violence Crime and Victims Act (2004)** section 54 refers to the disclosure of information to a relevant authority. This becomes important for a domestic violence survivor who has the right to make representation and receive information (under part 3, chapter 2) regarding a perpetrator convicted of a sexual or violent offence. The disclosure of information is permitted where a domestic violence survivor, or agency acting on behalf of a survivor, wishes to retrieve information from the relevant local probation board as to the licence or supervision requirements of the perpetrator, including details of hospital orders and conditions of release from hospital.

- **The Freedom of Information Act 2000**
- **Common law duty of confidence**
- **Section 37 and Section 39 Crime and Disorder Act.**

- **Housing Act (1985)** Section 84 (1) (schedule 2, ground 3) and amendments in 1996 (sections 144 and 145) give a local authority or housing association, or registered social landlords (RSLs) reasons for asking for information, namely to make enquiries as to whether to serve a possession order. This includes information relating to police visits, convictions and complaints against persons residing in the property regarding offences committed in the locality of the property. This provides the legal basis for

---

48 For further info see Home Office Prolific and other Priority Offenders Information Sharing Protocol.
http://www.crimereduction.gov.uk/ppo_protocol.doc
requests of information that may support eviction of a tenant who is a perpetrator of domestic violence. Local authority tenancy agreements should have a clause specifying that domestic violence by a tenant can be considered grounds for eviction.49

- **Housing Act (1996)** section 184 allows a partner organisation to make enquiries to establish whether an application is eligible for re-housing.50
- **Homelessness Act (2002).** Section 10 includes those that have been the subject of violence and harassment as ‘priority groups’ allowed for re-housing. This means that police held information regarding incidents of domestic violence and harassment recorded at the dwelling, as well as information of convictions against the perpetrators can be requested.51
- Also refer to the **Caldicott Principles** which set out a number of general principles that health and social care organisations should use when reviewing their use of client information.52

**Please note this list is not exhaustive.**

**Nb.** This legislation does not override existing legal safeguards on personal information. These safeguards are laid out in:

- **The Data Protection Act 1998**, for the processing of personal information.53
- **The Human Rights Act 1998**, for individual’s right to privacy.54

---

49 Directly quoted from Haringey’s Information Sharing Protocol.
50 Adapted from Ibid.
51 Directly quoted from Ibid.
52 A summary of the principles can be accessed here: http://www.tameside.gov.uk/tmbc8/principles.htm