



**Richmond Domestic Abuse Forum
Information Sharing Protocol for the Multi Agency Risk
Assessment Conference (MARAC)**

Agreed: June 2009

Review: June 2010

Reviewed and updated September 2010

Contents

Contents.....	2
Acknowledgements.....	2
Part 1 - Introduction.....	3
1.1 Purpose of this Protocol.....	3
1.2 Agencies covered by this agreement.....	4
1.3 Commitment.....	5
Part 2 – Data.....	6
2.1 Data to be shared.....	6
2.2 Information which may be disclosed.....	6
2.3 Non-personal data.....	6
2.4 Depersonalised data.....	7
2.5 Personal data.....	7
2.6 Sensitive personal data.....	8
Part 3 – Data Sharing.....	9
3.1 Statutory Gateways.....	9
3.2 Key principles governing disclosures made during or following a MARAC meeting.....	10
3.3 Local context for information sharing at MARAC.....	11
3.4 Consent.....	11
Part 4 – Process.....	13
4.1 The MARAC meeting.....	13
4.2 Information sharing outside of the MARAC.....	14
4.3 Information sharing with other MARACs.....	15
Part 5 - Security and Data Management.....	15
5.1 Data Controller and Responsibilities.....	15
5.2 Data Management.....	16
5.3 Disclosure requests.....	17
5.5 Breaches.....	18
5.6 Audit.....	18
Part 6 - Complaints.....	20
Appendix A: Signatories.....	21
Appendix B: Legal Framework Governing Information Sharing.....	24
Appendix C: Information Sharing Within Consent Form.....	34

Acknowledgements

This protocol was developed using guidance or protocols produced by CAADA and the London Boroughs of Greenwich and Lewisham

Part 1 - Introduction

1.1 Purpose of this Protocol

1.1.1 The Richmond MARAC (or 'Multi-Agency Risk Assessment Conference') has been running in Richmond since November 2007. The MARAC is a meeting that brings together representatives from a number of agencies in Richmond to share information about the highest risk victims of domestic abuse. The intention is that this will enable agencies to jointly develop and progress appropriate and timely actions to make the highest risk victims (and any children) safer and to reduce crime and disorder. The MARAC is coordinated by the Community Safety Partnership (for more information go to www.richmond.gov.uk/community_safety_partnership)

1.1.2 The objectives of the MARAC are:

- To share information to increase the safety, health and well being of victims, adults and their children;
- To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
- To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
- To reduce repeat victimization;
- To improve agency accountability; and
- Improve support for staff involved in high risk domestic abuse (DA) cases.

1.1.3 The purpose of this protocol is:

- To facilitate the exchange of information for this purpose;
- To clarify the understanding between signatories as to agencies responsibilities towards each other and data subjects;
- To facilitate information sharing for the purpose of domestic homicide reviews, subject to national guidance.

1.1.4 This protocol is not designed to replace any existing data sharing protocols in the borough, but rather to enhance arrangements relating specifically to the exchange of information regarding domestic abuse.

1.1.5 This protocol sits alongside the Operating Protocol for the Richmond Multi-Agency Risk Assessment Conference (MARAC) for high risk victims of domestic abuse.

1.2 Agencies covered by this agreement

1.2.1 The following agencies are permanent attendees at the MARAC and the Chief Officer (or designate) and are signatories to this Protocol (as contained in [Appendix A](#) of this document):

- DAIS (Drugs, Alcohol, Interventions, Support) and DIP (Drug Intervention Programme)
- EMAG
- LBRuT Adult and Community Services (ACS)
- LBRuT Children's Services and Culture (CSC)
- Metropolitan Police
- National Probation Service
- NHS Richmond (formerly Richmond and Twickenham Primary Care Trust)
- Refuge
- Richmond Churches Housing Trust (RCHT)
- Richmond Housing Partnership (RHP)
- South West London and St Georges Mental Health Trust (SWLSGT)
- Victim Support
- Welcare

1.2.2 Other agencies may be invited to permanent MARAC attendees or to provide information to the MARAC at a later date where the MARAC considers this would be appropriate.

1.2.3 Other agencies may be invited to attend or supply information to the MARAC where there is one or more cases being discussed where they can provide relevant information on the case and assist in the development and execution of the risk management plan.

1.2.4 Any agency attending on this ad hoc basis will be asked to sign the MARAC confidentiality declaration at the beginning of the meeting.

1.3 Commitment

By declaring a commitment to the procedures set out in this protocol, signatories:

1.3.1 Will ensure that they are aware of their own organisations information governance procedures

1.3.2 Will ensure that data sharing arrangements between them are in compliance with the legislation laid out in [Appendix B](#)

1.3.3 Pledge to consult periodically with each other upon matters of policy and strategy.

1.3.4 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 the purposes for which, and the manner in which, personal data are processed. The Data Controller will normally be the Designated Officer or Primary Designated Officer referred to in section 4 below.

1.3.5 Will not use the data received for any purpose other than that set out in this protocol, nor share it with any other party, without the disclosing partner's permission.

1.3.6 Undertake to ensure that they comply with all relevant legislation, this protocol, and any own internal policies on disclosure.

1.3.7 Agree to disclose information to relevant authorities under Section 115 of the Crime and Disorder Act 1998 - the police, local authority, probation or health authority, or to any persons acting on their behalf - where disclosure is for the purposes of a provision of the Act, and in accordance with any other relevant legislation. This agreement extends to those acting on behalf of a relevant authority to formulate or implement the Domestic Abuse Strategy.

1.3.8 Pledge 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. Each party also pledges to ensure that the data it holds is as accurate and up to date as possible.

1.3.9 Will seek their own legal advice, wherever necessary.

1.3.10 Any signatory may withdraw from this Protocol upon giving written notice to the other signatories. Data which is no longer relevant should be destroyed or returned. The partner must continue to comply with the terms of this Protocol in respect of any data that the partner has obtained through being a signatory.

Part 2 – Data

2.1 Data to be shared

Information may be shared at the MARAC about the following individuals:

- The victim(s) – this may include the new partner of a domestic violence perpetrator or previous partners;
- The children;
- The perpetrator (or alleged perpetrator); and
- Where relevant to the risks posed, members of the perpetrator's family or people with whom he/she has other relationships.

2.2 Information which may be relevant and be disclosed

Information may relate to the victims, children and/or perpetrator and anyone else judged to be at risk

- Name (including any aliases), date of birth, address(es), ethnicity, sexual orientation, gender, gender identity;
- Details of police call outs, arrests, prosecutions, Court Orders, injunctions, bail conditions and other legal issues including immigration status;
- Relevant information held by a member agency on recent contacts (e.g. meetings, interviews, sightings, phone calls). This will include information on behaviour, demeanour, attitude etc;
- Relevant information on previous contacts, including those which may have occurred outside the borough e.g. previous convictions, family or relationships history, substance misuse, mental health issues; and
- Any other information relating to the risks facing the victim and/or any other people who have been identified as being at risk.

2.3 Non-personal data

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

2.3.2 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.

2.4 Depersonalised data

2.4.1 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 post-code or address can reveal the identity of an individual. Signatories are also aware that it may be possible for an individual's identity to be revealed by comparing several sets of depersonalised data.

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

2.4.3 It is best practice at the time the data is collected to give subjects information about how anonymised data about them may be used.

2.5 Personal data

2.5.1 Signatory agencies understand that personal data is 'information which relates to a living individual who can be identified from that data'.

2.5.2 Personal data will be clearly marked and kept securely within a pass-worded computer system or otherwise physically secure with appropriate levels of staff access.

2.5.3 Signatory agencies undertake to destroy all personal data when no longer required for the purpose for which it was provided.

2.5.4 All grounds for the disclosure of personal information under this protocol will be formally recorded, and partners will process information fairly and objectively in every case.

2.5.5 Agencies agree only to 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.

2.5.6 Signatories undertake that schedule 2 of the Data Protection Act 1998 and the Freedom of Information Act will be satisfied where it is necessary to process personal data.

2.5.7 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 the victim or child(ren) in danger.

2.6 Sensitive personal data

Sensitive data is that which falls into any of the following categories:

- Criminal offences or proceedings;
- Racial or ethnic origin;
- Sexual life;
- Physical or mental health;
- Membership of a trade union; and
- Religious or spiritual beliefs.

Part 3 – Data Sharing

The success of the MARAC hinges on effective and timely information sharing. It is recognised that families experiencing domestic abuse, and particularly those at highest risk, will need the help and involvement of a wide variety of agencies. This may include input from agencies working in the social, welfare, economic, safety, housing, criminal and civil justice sectors. Because of this a partnership approach is vital. Individual agencies will hold incomplete information about the family and this can inhibit the development of the most appropriate approach to managing risk. In contrast sharing information through the MARAC facilitates the development of appropriate and timely risk management plans.

Information shared at the MARAC will be used to draw up a safety plan which will, in the light of the information available and when put into practice, attempt to address the risks faced by the victim and children. In some cases it may also cover the risks faced by other people such as family members, colleagues or friends. Risks faced by staff working with the family may also be identified and included in the action plan.

3.1 Statutory Gateways

The MARAC is just one of a number of different places where agencies will need to share information. Information sharing at the MARAC will take place within the framework provided by relevant legislation and guidance:

- Human Rights Act 1998
<http://www.opsi.gov.uk/acts/acts1998/19980042.htm>
- The European Convention on Human Rights
<http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>
- Data Protection Act 1998
<http://www.opsi.gov.uk/acts/acts1998/19980029.htm>
- Access to Health Records Act 1990
http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900023_en_1.htm
- Crime and Disorder Act 1998
<http://www.opsi.gov.uk/acts/acts1998/19980037.htm>
- Common Law Duty of Confidentiality¹
- Local codes or standards relating to confidentiality
<http://www.dca.gov.uk/foi/sharing/toolkit/lawguide.htm#part6>
- Caldicott Principles
<http://www.dh.gov.uk/assetRoot/04/06/84/04/04068404.pdf>

¹ Under the Common Law Duty of Confidentiality, information given or received in confidence or for one purpose should not be used for another or passed to a third party without their consent

- Confidentiality – NHS Code of Practice November 2003 (Dept of Health)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationPolicyAndGuidance/DH_4069253
- Freedom of Information Act 2000
<http://www.opsi.gov.uk/acts/acts2000/20000036.htm>
- Regulation of Investigatory Powers Act 2000
<http://www.opsi.gov.uk/acts/acts2000/20000023.htm>
- Children Act 1989
http://www.opsi.gov.uk/acts/acts1989/Ukpga_19890041_en_1.htm
- Children Act 2004
<http://www.opsi.gov.uk/ats/acts2004/20040031.htm>
- Adoption and Children Act 2002

Full details of how these pieces of legislation and guidance apply to information sharing within the MARAC are contained at [Appendix B](#) of this document.

3.2 Key principles governing disclosures made during or following a MARAC meeting

3.2.1 Decisions to disclose must be necessary and proportionate, taking into account:

- The prevention or detection of crime, including safeguarding someone's life and/or child protection needs;
- If it is in the public interest;
- The right to life and to live free from inhuman and degrading treatment and torture; and
- If it is needed in order for confidential counselling, advice and support to take place;

In summary, information can be shared provided each case brought to the MARAC meets the criteria outlined below:

3.2.2 Data Protection Act 1998

The prevention of crime exemption under the DPA means disclosure of information can be made to members of the same MARAC if it is necessary to prevent a crime against a named individual or a specified household.

3.2.3 Common law duty of confidence

An obligation of confidence exists where the individual has provided the information to another in circumstances where it is reasonable to assume that the provider of the information expected it to be kept confidential. Where there is a clear duty of confidence the information can only be disclosed to 'third parties' if there is informed consent, compulsion of law or public interest.

3.2.4 Human Rights Act 1998

A disclosure to members of the same MARAC will comply with the HRA if it:

- a) Is made for the purpose of preventing crime. Protecting the health and/or safety of alleged victims and/or the rights and freedoms of those who are victims of domestic violence and/or their children
- b) Is necessary for the purposes referred to in a) above and is no more extensive in scope than is necessary for these purposes
- c) Complies with all relevant provisions of law including the DPA and the Caldicott Guidelines

3.2.5 Caldicott Guidelines

The guidelines state that where an individual has not consented to the use of their information that wish will be respected unless there are exceptional circumstances. Such an exceptional circumstance is where there is a serious public health risk, risk of harm to the patient or other individuals or for the prevention, detection or prosecution of serious crime.

Practitioners should note that the Caldicott Guidelines are not law and that the DPA, HRA and common law will always take precedence.

3.3 Local context for information sharing at MARAC

3.3.1 Within the London Borough of Richmond upon Thames, the majority of agencies involved in the MARAC will be signatories to a number of local information sharing protocols will share information in accordance with this framework.

3.3.2 It is the responsibility of individual agencies and their representatives on the MARAC to be aware of any particular legislation and/or guidance affecting their ability to share information. They should also be aware of internal procedures within their agencies for information sharing particularly where there is any doubt over whether information can be shared within the MARAC.

3.3.2 This information sharing agreement for the MARAC operates alongside existing local information sharing protocols.

3.4 Consent

3.4.1 It should not be assumed that consent is essential in order for agencies to share information.

3.4.2 Obtaining consent remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought from and freely given by the data subject.

3.4.3 All agencies making referrals to the MARAC should have in place their own arrangements for ensuring that the victim and/or other family members where

relevant, are made aware of the circumstances in which information about them will be shared and with whom.

3.4.4 Agencies should explain to victims:

- About their (ex) partner's limited confidentiality and what information they may or may not have access to;
- About their own confidentiality;
- About the agency's child protection policy; and
- How information is shared between workers at different organisations and within the organisation.

3.4.5 However, in many cases the aims of the MARAC might be prejudiced if agencies were to seek consent. For example if it would put the victim at greater risk. 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 (see *section 3.2.1*).

3.4.5 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 (Section 2 (7) of the Children's Act 1989). Consent can be gained from only one person with Parental Responsibility, rather than both parents.

3.4.6 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.

3.4.7 Consent to share information will not be sought from the alleged perpetrator in order to protect the safety of the survivor. The perpetrator will not be informed about the meeting and the safety plan. Participants should take extraordinary care not to let the perpetrator know about any elements of the safety plan inadvertently.

3.4.8 Decisions to disclose without consent should be properly documented and identify the reasons why the disclosures are being made (i.e. what risk is believed to exist), the extent of any disclosures and the permitted use of the information.

3.4.9 Any decision to disclose information should conform to the principles set out in *section 3.2* above.

3.4.10 For any cases where a decision is made to refer to the MARAC without consent, agency will have to complete an *Information Sharing Without Consent Form*. A copy of this is at [Appendix C](#) or can be downloaded from www.richmond.gov.uk/domestic_abuse_multi-agency_risk_assessment_conference

Part 4 – Process

4.1 The MARAC meeting

4.1.1 At the beginning of each meeting (as laid out in *section 3.3* of the Operating Protocol for the Richmond MARAC) all agency representatives will sign up to the MARAC Confidentiality Declaration which is that:

‘Information discussed by the agency representative, within the ambit of this meeting is strictly confidential and must not be disclosed to third parties who have not signed up to the MARAC information sharing agreement, without the agreement of the partners of the meeting. It should focus on domestic abuse and child protection concerns and a clear distinction should be made between fact and opinion.

All agencies should ensure that the minutes are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to race, faith, gender, gender identity, sexuality and disability’

4.1.2 Any agency attending on this ad hoc basis will also be asked to sign the MARAC Confidentiality Declaration. These agencies may be invited to become permanent MARAC attendees or to provide information to the MARAC at a later date where the MARAC considers this would be appropriate

4.1.3 The information that is shared at the MARAC meeting will be used to construct a safety plan which will aim to address the risks faced by the adult victim and children.

4.1.4 Information on MARAC cases is sent out to members in advance of the meetings subject to the arrangements laid out in the Operating Protocol for the Richmond MARAC. No disclosures of information should be made to any other party, including the victim, without having been agreed at the MARAC. All decisions about how the information provided to the MARAC is to be used must be taken within the meeting. This includes both use by participants in the meeting and those outside the MARAC.

4.1.5 Cases coming before the MARAC will have been identified as being of the highest risk as defined by the MARAC referral threshold (as laid out in *section 4.3* of the Operating Protocol for the Richmond MARAC). A copy of the Risk Indicator Checklist and accompany guidance can be downloaded from www.richmond.gov.uk/domestic_abuse_multi-agency_risk_assessment_conference

4.1.6 The majority of cases will also involve children and so the requirement for information sharing for child protection purposes will, on most occasions, also come into force.

4.1.7 The MARAC covers only the highest risk cases of actual or suspected domestic abuse. Cases will generally be those where there is a threat of serious harm or homicide to the victim and/or her children. MARAC cases should therefore meet the criteria for information sharing without consent. For example most MARAC cases will clearly meet the 'exceptional circumstances' outlined in the Caldicott Guidelines.

4.1.8 Failing to share relevant information can put victims and their children at serious risk. Bearing this in mind decisions by agencies to disclose information must still be justifiable given the estimated level of risk and should be proportionate.

4.1.9 Professionals representing their agency on the MARAC should decide what information they should disclose on a case by case basis taking into account the criteria given above and their own agency guidance. A decision to disclose a particular piece of information can be made in the context of discussions within the MARAC and need not necessarily be decided beforehand. For example a victim may have made one or more visits to their General Practitioner or Accident and Emergency. These may become relevant and the decision taken to disclose if it emerges these occurred around the same time as the police attended domestic violence incidents.

4.2 Information sharing outside of the MARAC

4.2.1 It may be the case that in order to implement certain elements of the MARAC action plan to manage risk persons who are not signed up to the MARAC information sharing protocol may need to be informed of certain facts. For example a perpetrator's name could be disclosed to a caretaker so that he would not be admitted to certain premises but the reason would not be given.

4.2.2 This is addressed in *section 7.7* of the Operating Protocol for the Richmond MARAC.

4.2.3 Considerations here are similar to those for sharing information within the MARAC. The risk of crime must be genuine or likely. If this is the case the Data Protection Act allows only the minimum necessary information to be disclosed by a MARAC agency to non MARAC recipients to allow a crime to be prevented.

4.2.4 Disclosures to persons outside the MARAC can still be permitted under the Human Rights Act. However members should satisfy themselves in advance that such disclosures are strictly necessary for the purpose for which they are being made.

4.3 Information sharing with other MARACs

4.3.1 In deciding whether to disclose information to another MARAC the principles set out in part 2 and 3 should be adhered to. This is addressed in *section 7.8* of the Operating Protocol for the Richmond MARAC.

4.3.2 The initial disclosure by the referring MARAC should be restricted to the victim or perpetrator's name (and any children) and the fact they have been discussed at the Richmond MARAC. Recipient MARACs should have an information sharing protocol in place. Provided this is the case the Richmond MARAC will consider what additional information should be passed on, deciding what it can disclose and properly document the reasons for disclosure, what information will be disclosed and what restrictions are placed on the use of that information. This can include the completion of a referral form where requested by the recipient MARAC.

4.3.3 For urgent cases, occurring outside the MARAC meeting process, this action will be delegated to the Domestic Abuse coordinator or MARAC Administrator.

Part 5 - Security and Data Management

5.1 Data Controller and Responsibilities

5.1.1 Designated officers

Each signatory agency must appoint a Primary Designated Officer who will be a manager of sufficient standing and have a co-ordinating and authorising role. Agencies may also appoint further Designated Officers within the same body.

5.1.2 Responsibilities

Specific responsibilities will be:

- Ensuring their agency abides by the sections of this protocol;
- Ensuring that all Designated Officers and other staff are fully aware of their responsibilities;
- Appointing other staff in the body 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 the partner's 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 and Primary Designated Officers are responsible for ensuring that processing of personal data is in accordance with the principles of the Data Protection Act 1998, namely:

- It is obtained, processed and disclosed fairly and lawfully;
- Kept securely;
- Processed in accordance with the rights of the data subjects;
- Accurate, relevant and held no longer than necessary;
- Disclosed only for a specified related purpose;
- Disclosed without the subject's knowledge and/or agreement only where failure to do so would prejudice the objective.

Designated Officers and Primary Designated Officers are responsible for keeping informed the data owners for each signatory agency. Only they can make formal requests and document agreements for the sharing of personal information under this 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.

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 folder or file, which must be kept up to date and include;

- Record of data disclosed;
- Project chronology;
- Project access list;
- Notes of meetings with partners;
- Recent correspondence and phone calls

5.2 Data Management

5.2.1 Partner agencies agree that it is their responsibility as signatories to this Protocol to ensure that they have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information we hold.

5.2.2 Partner agencies understand that there measures need to be taken to ensure the security of our partners and to protect the general public. It is the responsibility of each signatory to the agreement to ensure that their staff and any individual having access to information produced as a result of the MARAC receive sufficient training to enable them to handle such information and have been vetted to a satisfactory standard.

5.2.3 Personal information must be;

- Shared via Secure eMail using GCSX or the CJSM service² when transmitted electronically. All partner agencies are responsible for ensuring they have this

² Criminal Justice Secure Mail (CJSM) exists to send confidential information by email to other organisations, which are also members of the secure email system. This service is run by the government's Criminal Justice Service on behalf of any public authorities, such as local authorities

facility. The MARAC Administrator will maintain list of the contact details of agency representatives, including their Secure eMail address.

- Be protected by back-up rules.
- When stored on a computer system be password protected or stored with restricted access.
- When manual, be stored in a secure filing cabinet when not in use.
- When manual, once paper copies have fulfilled their use they must be disposed of as confidential waste by shredding or other secure means.
- When manual, be located in a geographically secure environment.
- Not be inputted or accessed without industry standard devices as defined by BS7666.

5.2.4 All data held for the purposes of the MARAC is subject to a specified shelf-life of 3 years. Each agency that attends MARAC can hold relevant information for as long as a risk to the victim or children remains. The information retained should be proportionate to the perceived risk. All personal data disclosed will be held for this period. Particular care must be taken when agencies are disposing of old hard drives that have been used to store information relating to the MARAC. A suitably approved device must be used to wipe the memory clear or the hard drive must be physically destroyed to prevent third parties gaining access to this sensitive information.

5.3 Disclosure requests

5.3.1 Agreed procedures will generally require making a request in writing.

5.3.2 Access to information obtained through this protocol other than Primary Designated Officers and Designated Officers should be limited to employees whose work is directly related to the aim for which the data was obtained and those working within the crime reduction programme or field.

Subject Access Request

5.3.3 The data subject is legally entitled to request their records from the receiving agency under the Data Protection Act 1998, unless an exemption applies. If a subject requests access to their records the receiving agency should contact the disclosing agency to determine whether the latter wishes to claim exemption. From this stage the procedure should be fully documented in writing and stored on file.

Weeding of data

and health agencies, which have occasional links with the justice system. Organisations within the justice system itself (e.g. the Police and Probation Service) are already part of the Government Secure Community. For more information, go to <http://www.cjsm.cjit.gov.uk/>

To use Secure eMail you must be using an email account from an organization within the Government Secure Community (e.g. .gsx, .gsi or .pnn); or an organization signed up to Secure eMail or anyone with an address ending .nhs.net

5.3.4 Signatories to the protocol must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice. Partners must agree a maximum retention period for data.

5.4 Publication

5.4.1 Where possible, this protocol should be published and made available to the general public for clarity of purpose. This publication will be subject to a regular review of information sharing protocols.

Media handling

5.4.2 Signatories agree when handling 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 agree:

- to be fair to our fellow signatory agencies, and maintain their integrity;
- when providing information to the public, to do so honestly and fairly;
- statements must reflect the multi-agency decision process;
- consent of the data owner will be sought prior to release to the media;
- where practical, individual data subjects will be consulted if the media coverage was such that it may identify the individual.

5.4.3 This might be best achieved through development of a media strategy on a case-by-case basis, co-ordinated by the data owner.

5.5 Breaches

5.5.1 Partner agencies undertake at all times to comply with data protection and other legal requirements relating to confidentiality.

5.5.2 Partner agencies agree that any breach of confidentiality will seriously undermine and affect the credibility of the MARAC and broader partnership and information sharing arrangements and render us liable for breach of the law.

5.5.3 Any security breaches will be reported to the Chair of the MARAC, who is responsible for monitoring these. All agencies must have internal disciplinary policies in place for dealing with security breaches.

5.5.4 All parties to this agreement are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

5.6 Audit

5.6.1 Partner agencies will ensure that they will collect, process, store and disclose all data held within the terms of the Protocol and the relevant legislation. Partner

agencies agree to ensure that all information held is accurate, relevant and fit for the purpose for which it is intended.

5.6.2 Partner agencies agree to store all held data as securely as per the terms of Part 3 'Security'. Partner agencies pledge to conduct regular audits of their security arrangements to ensure they are effective.

5.6.3 The Community Safety Partnership undertakes to conduct annual audits of this protocol in order to amend it and ensure it remains fully effective

Part 6 - Complaints

6.1.1 Initial complaints must be referred to the appropriate Primary Designated Officer or Designated Officer.

6.1.2 The procedure to be followed in the event of a formal complaint being received is

- That the Chair of the MARAC is to be informed;
- 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 of our partners;
- Partner agencies will undertake to do all we can within the guidelines of the Data Protection Act 1998 to assist with any complaint.; and
- Individuals do retain the right to raise a complaint with such bodies as the Information commissioner or statutory ombudsman.

6.1.2 Initial complaints by one signatory agency against another signatory agency about their activity or processes must be referred to the Chair of the MARAC and the procedure to be followed in the event of such a complaint being received is as follows:

- Any formal complaint by a signatory regarding any stage of the process will be referred to the Community Safety Partnership Strategic Group
- Partner agencies will undertake to do all we can within the guidelines of the Data Protection Act 1998 to assist with any complaint.
- Individuals do retain the right to raise a complaint with such bodies as the Information commissioner or statutory ombudsman.

Appendix A: Signatories

The Chief Officers (or designate) formally agree to the following as permanent attendees at the MARAC:

- to subscribe to the principles contained in the Protocol;
- to work to the procedures identified within the Protocol
- to fully implement the protocol within their own agency, ensuring all staff know of its existence to support the MARAC, and to support their attendance at any training event required;
- to supply information within the bounds of this Protocol at no financial cost to any of the other signatory agencies; and
- to contribute to the development of trust and confidence between the signatory agencies by working within the framework of the protocol and Operating Protocol for the Richmond MARAC to disclose, retain and dispose of data for the purpose of supporting the MARAC.

DAIS (Drugs, Alcohol, Interventions, Support) and DIP (Drug Intervention Programme)

Name	
Signature	
Date	

EMAG

Name	
Signature	
Date	

LBRuT Adult and Community Services (ACS)

Name	
Signature	
Date	

LBRuT Children’s Services and Culture (CSC)

Name	
Signature	
Date	

Metropolitan Police

Name	
Signature	
Date	

National Probation Service

Name	
Signature	
Date	

Refuge

Name	
Signature	
Date	

NHS Richmond (Formerly Richmond and Twickenham Primary Care Trust)

Name	
Signature	
Date	

Richmond Churches Housing Trust (RCHT)

Name	
Signature	
Date	

Richmond Housing Partnership (RHP)

Name	
Signature	
Date	

South West London and St Georges Mental Health Trust (SWLSGT)

Name	
Signature	
Date	

Victim Support

Name	
Signature	
Date	

Welcare

Name	
Signature	
Date	

Appendix B: Legal Framework Governing Information Sharing

The Home Office guidance document “Safety and Justice: sharing personal information in the context of domestic violence – an overview”, published in 2004, identifies a number of questions that need to be considered in any case where a public sector body proposes to share information, as follows.

- Does the body have a legal power to share the information?
- Would the information sharing comply with the Human Rights Act 1998?
- Would there be a breach of a common law duty of confidentiality?
- Would there be a breach of the Data Protection Act 1998?

These four issues are addressed below. Other relevant legal provisions are also considered.

The first issue is likely to be relevant to public sector bodies (in general, these cannot do anything unless they have an express or implied statutory power to do so). The second issue is relevant to public sector bodies, as they have a specific duty under the Human Rights Act 1998 not to act in breach of the human rights that are set out in the European Convention. Private or voluntary sector bodies are not subject to a specific statutory duty of this nature, but as a matter of good practice they will no doubt seek to act consistently with the Convention. The third and fourth issues are relevant to both public and private or voluntary sector bodies.

1.1 Legal Power to share information

- a) The Crime and Disorder Act 1998 (CDA) aims to tackle crime and disorder and help create safer communities.
 - Section 115 of the CDA provides a power (but not an obligation) for information sharing between ‘responsible’ public bodies (e.g. police, local authority, health authority) and with ‘co-operating’ bodies (e.g. DV support group, victim support group) participating in the formation and implementation of the local crime and disorder strategy. This must be to pursue a specific objective within the strategy and be subject to a written agreement.
 - In addition, Section 115 stipulates that any person who would not have power to disclose information to a relevant authority or a person acting on behalf of such an authority shall have power to do so in any case where

the disclosure is necessary or expedient for the purposes of any provision of the Act.

- This power must be exercised in accordance with any other relevant legislation, including the HRA, common law of confidence and the DPA (see below).

b) The Children Act 1989 (CA) redefined the law around child welfare and introduced new measure for working with children and families. Key principles include:

- The child's welfare is paramount.
- Professionals will work in partnership with the child, with other professionals and with the parents and significant others.
- Section 27 stipulates that where it appears to a local authority that any authority or other person mentioned in subsection (3) (see below) could, by taking any specified action, help with the exercise of any of their functions under this part, they may request the help of that other authority or person, specifying the action in question. An authority whose help is so requested shall comply with the request if it is compatible with their statutory duties and obligations and does not unduly prejudice the discharge of any of their functions.

Agencies listed in subsection 3 are:

- a) Any local authority;
 - b) Any local education authority;
 - c) Any local housing authority;
 - d) Any health authority; and
 - e) Any person authorised by the Secretary of State for the purposes of this section.
- Section 47 places a duty on the above authorities to assist with enquiries (in particular by providing relevant information or advice) if called upon by the authority conducting enquiries following reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm.

c) Children Act 2004

- Section 10 establishes a duty on Local Authorities to make arrangements to promote co-operation between agencies in order to improve children's well-being, defined by reference to the five outcomes and a duty on key partners to take part in those arrangements. It also provides a new power to allow pooling of resources in support of these arrangements.
- Section 11 creates a duty for the key agencies who work with children to put in place arrangements to make sure that they take account of the need to safeguard and promote the welfare of children when doing their jobs.

- d) Adoption and Children Act 2002 (ACA) modernises the law on adoption in line with the Children Act 1989.
- Section 120 amends Section 31 (9) of the Children Act 1989 to extend the definition of harm to include “impairment suffered from seeing or hearing the ill-treatment of another”.

1.1 Human Rights Act 1998

The Human Rights Act 1998 (HRA) gives further effect in UK law to the European Convention on Human Rights (ECHR). The ECHR contains fundamental rights and freedoms such as the right to life, the right to a fair trial and freedom of thought, religion and speech and respect for private and family life.

- Article 2.1 stipulates that “Everyone’s right to life shall be protected by law”.
- Article 3 stipulates that “No one shall be subjected to torture or to inhuman or degrading treatment or punishment”.
- Article 6 stipulates the right to a fair trial.
- Article 8 stipulates that “Everyone shall have the right to respect for his private and family life, his home and correspondence..... There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

Articles 2.1 and 3 may create a duty on public sector bodies to share information in order to protect individuals from serious threats to their physical safety or wellbeing.

On the other hand, article 8 may prohibit public sector bodies from sharing personal information in cases where such sharing cannot be justified as being necessary for one of the objectives listed in article 8.2.

1.3 Common Law relating to Confidentiality

The common law protects against the disclosure of information (whether personal or not) given in ‘confidential’ contexts.

- Breach of confidence may be demonstrated where the information:
 - Has a ‘quality of confidence’ (i.e. is not already in the public domain and has sensitivity and value);
 - Is given in circumstances giving rise to an ‘obligation of confidence’ on the part of the person to whom the information has been given (e.g. nurse/patient);

- Is used in a way that was not authorised.³
 -
- However the duty of confidentiality is not absolute. Disclosure can be justified if:
 - The information has ceased to be confidential in nature (for instance, because it has come into the public domain);
 - The person to whom the duty is owed has consented to the disclosure;
 - There is an overriding public interest in disclosure;
 - Disclosure is required by a court order or other legal obligation.⁴

Where explicit consent has been obtained for sharing the information between the agencies, then any duty of confidence will not prevent the sharing of information in line with the given consent.

When there is no explicit consent, or when the explicit consent does not cover specific information given in confidence, then the information will not be shared unless one of the conditions under Schedule 2 and (where appropriate) Schedule 3 of the Data Protection Act 1998 is met. These conditions are discussed in detail below. In cases where information is shared about individuals who pose a high risk of harm to their partners or children, or about high risk victims/survivors and their children, then if the appropriate conditions in Schedule 2 and/or 3 are met then there in many cases there will also be a public interest defence to any claim for breach of confidence. However, partner agencies may need to take their own advice in specific cases.

If the information is shared without explicit consent then the basis of the decision to share the information together with the details of who the information was shared with must be recorded as part of the case file.

³ Department for Constitutional Affairs (2003). Public Sector Data Sharing: Guidance on the Law. London: Department for Constitutional Affairs.

⁴ Department of Health (2003). What to Do if You're Worried a Child is Being Abused. London: Department of Health.

1.4 Data Protection Act 1998 (“DPA 1998”)

DPA 1998 contains a set of eight data protection principles. “Data controllers” – i.e. persons who control the processing of personal data – must comply with these principles in relation to such processing. Sharing personal data would constitute “processing” for the purposes of the Act. The eight principles are discussed below, in turn.

First Principle

The first Data Protection principle states that data must be processed lawfully and fairly. Further, at least one of the conditions in Schedule 2 to the Act must be satisfied; and in addition where sensitive personal data is processed at least one of the conditions in Schedule 3 must be satisfied.

Lawful processing

In order for data to be processed lawfully: (i) if the data controller is a public authority then it must have an express or implied statutory power, or other legal power, enabling it to act in this way: (ii) the processing must not breach HRA 1998; and (iii) the processing must not breach the common law duty of confidence. These issues were discussed above.

Fair Processing

- a) In most cases the consent of the survivor to share her/his personal and sensitive data will be sought. Where consent is sought, the form used to obtain explicit consent for information sharing must clearly indicate how the information given will be processed and will also include a fair processing statement.
- b) Where it is not possible to provide a fair processing notice of the survivor before sharing information, partner agencies will ensure that the MARAC representatives are practitioners competent to make a judgment on whether it is nevertheless permissible to share the information, on the basis of the crime prevention exception in section 29 of DPA 1998.
- c) Consent to share information will not be sought from the alleged perpetrator in order to protect the safety of the survivor, and fair processing information will not usually be provided to alleged perpetrators. Where information about alleged perpetrators has been provided by the perpetrators themselves, and no fair processing information has been provided to them, then a judgment will need to be made on whether it is nevertheless permissible to share the information, on the basis of the crime prevention exception in section 29 of DPA 1998. Where information about alleged perpetrators has been provided by third parties (e.g. by survivors) a judgment will need to be made as to whether it is practicable to provide fair processing information to the alleged perpetrators before sharing that information. If not, then the absence of a fair processing notice does not prevent

information sharing from taking place. Partner agencies will need to ensure that MARAC representatives are practitioners competent to make a judgment on these issues.

- d) Where information about the alleged perpetrator is shared, this will be done on a 'need to know' basis only, i.e. the minimum information consistent with the purpose for sharing will be given.

Schedule 2, Data Protection Act 1998

The sharing of personal data under this agreement will meet schedule 2 of the Data Protection Act because either the individual will have given explicit consent, or the information will only be shared in order to protect the vital interests of the data subject (Para 4) or the processing is necessary for the administration of justice or for the exercise of any functions conferred on any person by or under any enactment (Para 5). Consent to share information on the alleged perpetrator will not be sought since to do so is likely to increase risk to the survivor and her/his children.

Schedule 3, Data Protection Act 1998

The sharing of sensitive personal data under this agreement will meet schedule 3 of the Data Protection Act because either:

- The data subject has given explicit consent to the processing; or
- The processing is necessary to protect the vital interests of the data subject or another in cases where consent cannot be obtained; or
- The processing is necessary for the administration of justice or for the exercise of any function conferred on any person by or under any enactment; or
- The processing comes within the order⁵ made by the Secretary of State in 2000 under paragraph 10 of Schedule 3, in that it is: (a) in the substantial public interest; (b) necessary for the purposes of the prevention or detection of any unlawful act (or failure to act), and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those [crime prevention/detection] purposes.

Second Principle

Personal data shall be obtained only for the specified and lawful purpose set out in this agreement, and shall not be further processed in any manner incompatible with that purpose.

⁵ See SI 2000/417, Schedule, paragraph 1.

Any information shared at the MARAC will be collected for the purpose of this Agreement and will be used only for a purpose compatible with the purpose of this Agreement.

Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- a) This agreement covers the sharing of case information on a 'need to know' basis, and therefore only information relevant directly to the specified purpose of this agreement will be shared.
- b) In general, if consent for sharing has been given by the survivor, then there is no need to undertake a detailed analysis of the exact need of the requestor followed by a subsequent editing of the case file to share only exactly the information required. To do this on each occasion would be impractical.
- c) However, care will be taken to ensure that explicitly confidential information is not shared inappropriately. In particular survivors may give consent to share all information except for some particularly confidential information. In this circumstance there is no consent to share this confidential information and so it should not be shared unless there is a public interest to do so.
- d) If consent for sharing has not been given by or sought from the survivor, or if the information pertains to the alleged perpetrator (and therefore consent has not been sought) information should be shared only on a 'need to know' basis where it meets the specific purpose of this Information Sharing Agreement within the terms of the Crime and Disorder Act 1998 and/or the Human Rights Act 1998.

Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

- a) The information to be shared under this agreement is subject to each agency's normal validation procedures to ensure data quality.
- b) If any partner agency becomes aware of an error in the shared information or a change in the shared information they must notify the other partner agencies of this change as soon as practical to ensure that all agencies' copies of the information remain accurate and up to date.

Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

- a) The co-ordinating agency of the MARAC will, notwithstanding the fifth data protection principle, keep records of the cases dealt with by the MARAC along with any action plans and implementation notes.
- b) Records pertaining to each individual agency's involvement with a MARAC case will be held for as long as required by the agency's respective record retention schedule, and then securely destroyed.

Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act.

- a) This agreement in no way alters the rights of individuals under the Data Protection Act 1998, the Human Rights Act 1998 or under the common law Duty of Confidentiality. However, partners to this agreement will not routinely divulge information gained for the purposes of this agreement to the alleged perpetrator or his/her agents. Requests for this information will be considered by the MARAC meeting on a case by case basis with consideration being given to the use of the 'crime and taxation exemption' section 29 of the Data Protection Act 1998. The Information Commissioner has stated that where relying on this exemption, there would need to be a substantial chance, rather than a mere risk, that in the particular case the purposes (here the prevention of crime) would be noticeably damaged by failure to process. The MARAC will document the decision taken and the reasons for the decision to process the data or not.
- b) Partners to this arrangement will respond to any notices from the Information Commissioner that imposes requirements to cease or change the way in which data is processed.
- c) Partners will comply with subject access requests in compliance with the relevant legislation.

Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- a) Information shared at the MARAC meetings will not be taken outside the meeting unless the agency has an active role in the action plan for enhancing the safety of the survivor and her/his children or is already providing services to or is involved in ongoing case work in respect of the survivor, her/his children and/or the alleged perpetrator.
- b) Personal information provided to the partner agencies of the MARAC prior to the MARAC meeting for the purposes of research will be securely destroyed

immediately the partner agency is able to verify that it holds no information on any of the parties named.

- c) As the information being shared under this agreement is only information that is directly relevant to the specific purpose of the agreement, each partner agency with an active role in the action plan for enhancing the safety of the survivor and her/his children or who is already providing services to or is involved in ongoing case work in respect of the survivor, her/his children and/or the alleged perpetrator will keep a record of that information along with their other records relating to the case.
- d) All information relating to individuals who are receiving services from any of the partner agencies must always be managed securely when held by either agency.
- e) The physical transfer of information between agencies will always be undertaken in a secure manner to ensure that the information is only ever accessibly to the individuals within the organisation who 'need to know' the information.

Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

- a) All of the signatories to this agreement are inside the European Economic Area.

1.5 Other relevant legal considerations

The Freedom of Information Act 2000 (FOIA) enables any member of the public to apply for access to information held by bodies across the public sector. The legislation will apply to a wide range of public authorities, local authorities, health trusts, doctors' surgeries and other public organisations.

- The Act provides a general right of access to information held by public authorities in the course of carrying out their public function, subject to certain conditions and exemptions. Alongside other legal protections, the exemptions provide grounds for refusal to provide information. These exemptions would need to be considered where a request was made under the Act by alleged perpetrators for information about survivors of domestic violence.
- Sections 22-44 of FOIA contain the exemptions, which include:
 - Information held in relation to the investigation, prevention, detection or prosecution of a crime, or the apprehension of offenders, or the administration of justice.

- Information held as court documentation.
- Information that constitutes personal data, in cases where disclosure would breach any of the data protection principles.
- Information the disclosure of which would constitute a breach of confidence.
- Information for which legal professional privilege exists.

Some of these exemptions are absolute. Others are subject to a public interest test, requiring consideration of whether the public interest in maintaining the exemption outweighs the public interest in disclosure.

Appendix C: Information Sharing Within Consent Form

Victim name and DOB				
Children	DOB	Relationship to perpetrator	Address	School (If known)

Concern

	Immediate risk / crisis	Risk identified through risk assessment
Child(ren) at risk/Danger to child(ren)		
Danger to client		
Client poses a risk to self or others		
Risk Identification Checklist (number of ticks)		
Incident/information causing concern (include source of information)		

Legal Authority to share

Protocol relevant _____ OR

Legal grounds (please tick 1 or more grounds below)

Prevention and detection of crime (Crime and Disorder Act 1998)

Prevention/detection or crime and/or apprehension or prosecution of offenders (DPA, s. 29)

To protect vital interests of the data subject; serious harm or matter of life or death (DPA, Sch. 2 & 3)

For the administration of justice (usually bringing perpetrators to justice (DPA, Sch. 2 & 3)

For the exercise of functions conferred on any person by or under any enactment (police/social services) (DPA, Sch. 2 & 3)

In accordance with a court order

Overriding public interest (Common law)

Child protection – disclosure to social services or police for the exercise of functions under the Children Act, where the public interest in safeguarding the child's welfare overrides the need to keep the information confidential (DPA, Sch. 2 & 3)

Right to life (Human Rights Act, Art. 2 & 3)

- Right to be free from torture or inhuman or degrading treatment (Human Rights Act, Art. 2 & 3)

Balancing Considerations

- Pressing need
- Respective risks to those affected
- Risk of not disclosing
- Interest of other agency/person in receiving it
- Public interest in disclosure
- Human rights
- Duty of confidentiality

Comments	
Internal consultations (Names, dates and advice/decisions)	
External consultations (Home Office guidance, Information-sharing Helpline)	

Client notification

Client notified of disclosure(s)?	Yes/No	Date of notification	<i>Please insert date of disclosure</i>
If not, why not?			

Review

Date for review of this situation (Review to include feedback from the agencies informed as to their response)	Yes/No	Date of notification	<i>Please insert date of disclosure</i>
Who is responsible for ensuring the situation is reviewed by this date.			

Record following details of information sharing in case file:

- Date info shared; Agency and named person informed; Method of contact (by email, letter, phone call); Legal authority for each agency

Signed and dated by caseworker

Authorised and dated by manage