Protective Marking	Not Protectively Marked
Suitable for Publication Scheme? Y/N	Yes
Title and version	Wandsworth Multi-Agency Risk Assessment Conference (MARAC) ISA
Summary	Information Sharing Agreement for MARAC meetings
Author and warrant / pay number	C100487 Natalie BLAGROVE
Creating Branch, Code and OCU	Wandsworth
Date created	07/06/2012
Review Date	06/06/2013

Information Sharing Agreement

An agreement between partners in the Multi-Agency Risk Assessment Conference (MARAC) for the London Borough of Wandsworth to support the sharing of information between MARAC partners about victims of domestic violence at high risk of harm

Document History

This document has been distributed to:

Date	Released to	Title	Agency	Comments
07/06/2012	David Chinchen	Borough Commander	Wandsworth Borough Police	Signed
07/06/2012	Paul Martin	Chief Executive	Wandsworth Borough Council	Signed
07/06/2012	Derec Craig	Senior Service Delivery Manager	Victim Support	Signed
07/06/2012	Mike Terry	Assistant Chief Officer	London Probation	Signed
07/06/2012	Lech Bogdanowicz	Information Governance Manager	St George's Healthcare NHS Trust	Signed
07/06/2012	John Hughes	Information Governance Manager	South West London & St George's Mental Health NHS Trust	Signed
07/06/2012	Lesley Bounds	Borough Manager	Wandsworth Integrated Drug & Alcohol Service (IDAS)	Awaiting Signature
07/06/2012	Lyndsey Dearlove	Manager	Wandsworth Women's Aid	Signed
07/06/2012	Colin Lyden	ASB Manager	Veridian Housing	Awaiting Signature (email sent)
07/06/2012	Andy Meekings	Senior Worker	Metropolitan Housing Trust	Signed

CONTENTS

1. PURPOSE OF THE AGREEMENT

This Individual Information Sharing Agreement has been developed to:

a) Define the specific purposes for which the signatory agencies have agreed to share information.

b) Describe the roles and structures that will support the exchange of information between agencies.

c) Set out the legal framework within which the information is shared, including reference to legal powers to share information, the Human Rights Act 1998, the common law duty of confidentiality, the Data Protection Act 1998, and other relevant legal considerations.

d) Describe the security procedures necessary to ensure compliance with responsibilities under the Data Protection Act and agency specific security requirements.

e) Describe how this arrangement will be monitored and reviewed.

The signatories to this agreement will represent the following agencies/bodies:

- Wandsworth Borough Police, Metropolitan Police Service
- London Probation Service (Wandsworth)
- Wandsworth Borough Council
- Wandsworth Borough Victim Support Service
- South West London & St George's Mental Health NHS Trust
- St George's Healthcare NHS Trust
- Wandsworth Integrated Drug & Alcohol Service (IDAS)
- Wandsworth Women's Aid
- Veridian Housing Association
- Other agencies identified as relevant by the MARAC co-ordinator and/or MARAC partners on a case-by-case basis

Other agencies may be invited into full membership of the MARAC or to provide information to the MARAC at a later date where the MARAC considers this would be appropriate.

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.

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

2. SPECIFIC PURPOSE FOR SHARING INFORMATION

a) In order to meet the full range of social, welfare, economic, safety, accommodation, criminal and civil justice needs that individuals living with or escaping domestic violence have, a multi-agency partnership approach is required (see the Home Office report[1]).

b) The Crime and Disorder Act (1998) places this obligation on a statutory footing, requiring some organisations to form partnerships to tackle crime and disorder, including domestic violence, and provides a legal power to share information (Home Office report).

c) Responsible information sharing plays a key role in enabling organisations and professionals to protect domestic violence victims and their children and to save lives. Casework, advocacy, conducting risk assessments and providing general support and protection may all require information about individuals to be shared with other agencies. Indeed, Articles 2 and 3 of the Human Rights Act (1998) (HRA) place an obligation on public authorities to protect people's right to life and their right to freedom from torture and inhuman and degrading treatment. Meeting these obligations may necessitate lawful information sharing.[2]

d) This information sharing protocol relates specifically to the multi-agency group responsible for conducting the Multi-Agency Risk Assessment Conference (MARAC). Partner agencies to the MARAC will share information specifically for the purpose of making or modifying and implementing plans to support the reduction of future harm for very high risk domestic violence victims and their children.

Management Summary

a) This agreement details the legal basis by which the partners, within the context of the MARAC, can share personal and sensitive information about victims of domestic violence, the alleged perpetrator and any children of the parties for the purpose of responding to the safety needs of victims and their children at very high risk of harm.

b) The agreement covers situations where consent has been explicitly given and recorded.

c) The agreement also covers the necessary process for sharing information when consent has not been explicitly given, or has not yet been recorded.

[1] See the Home Office Report 30 – see Appendix 1 at the end of this document.
[2] Taken from the Home Office Report 30

d) The agreement does not cover the legal basis for sharing of case information with any other agency other than those listed as signatories to this agreement.
e) The agreement does not cover the legal basis for the sharing of information that is not expressly for the purpose of responding to the safety needs of victims of domestic violence at high risk of harm.

Objectives

What are the objectives of the partnership?

a) To share a common objective of reducing future harm to clients and/or their children at high risk due to domestic violence.

b) To share a common objective to deliver Wandsworth's Domestic Violence Strategy 2012-2015.

c) To support the Domestic Violence Strategy to reduce domestic violence so that children, women and men do not suffer as a consequence and, where domestic violence does occur, to improve our response to both victims and their children, and to perpetrators.

d) To support the Domestic Violence Strategy to improve co-operation and joint action across the key partnership agencies in order to facilitate safe and consistent policy and practice responses to victims and perpetrators of domestic violence ensuring that the needs of all members of our diverse communities are considered.

e) To develop standardised domestic violence protocols and guidance, covering such areas as information sharing, referrals and risk assessment.

f) To develop the MARAC (Multi-Agency Risk Assessment Case Conference) alongside the development of the independent advocacy service.

Partner Agencies Benefits

a) This agreement provides legal clarity for all staff within the partner agencies who are working together to reduce future harm to clients at high risk due to domestic violence and allow agencies to feel confident that they can provide a comprehensive, safe, quality service to clients within the provisions of the law.

b) Consequently, this agreement should enable members of the MARAC to make or modify plans, in the light of information shared, which better support the victim in enhancing her/his safety and that of her/his children.

c) This agreement will support increased mutual understanding of domestic violence issues and the use of risk assessment techniques as well as increasing partners' knowledge of the success of different types of intervention strategies.

d) This agreement will assist in avoiding the duplication of effort in respect of service provision and record taking.

e) This agreement will enhance the reputation of signatory agencies for professionalism and credibility with clients and other agencies by demonstrating their competence in this area.

Citizen Benefits

This agreement will enable:

a) Timely action to be taken to protect victims and children from further abuse.

b) Comprehensive risk identification and safety planning based on a full account of the facts and circumstances of each victim's situation.

c) 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 victim's needs and history, including other service contact and use.

d) Victims to avoid the added distress of having to repeat details of their history or experience of domestic violence and other circumstances each time they encounter a different service.

e) This agreement will also help re-assure citizens that their personal information is being handled securely and only being used as necessary to ensure that the partners are able to deliver services effectively in order to enhance the safety of victims of domestic violence and their children.

f) Wandsworth Victim Support Service, or another identified agency, to act as the advocate for the victim at the MARAC and provide for two-way communication between the MARAC and the victim.

How will this information sharing arrangement further those objectives?

a) It is now recognised that in order to meet the full range of social, welfare, economic, safety, accommodation, criminal and civil justice needs that individuals living with or escaping domestic violence have, a multi-agency partnership approach is required (Hague, 2000; Humphreys, *et al*, 2001; Home Office, 2003). In general, individual agencies hold incomplete information about the circumstances surrounding a victim of domestic violence, which may lead to inappropriate or untimely interventions. Sharing information through the MARAC enables agencies to act from a better factual understanding of the situation and of the risks faced by the victim and her/his children.

b) At the MARAC meeting, partners to this Agreement will ensure that they are fully prepared to share all relevant information known to the agency on the circumstances surrounding the victim and her/his children.

c) At the MARAC agencies will discuss the likely outcomes of the proposed action plan to ensure that their combined actions are likely to promote the safety of the victim and her/his children.

d) By sharing their understanding of risk in particular situations, agencies are in a better position to integrate risk assessment into their daily practice.

e) Wandsworth Victim Support Service, or another identified agency, will represent the interests of the victim and take any suggested action back to the victim for her/his consideration.

Information to be shared

The following information will be shared

a) The information to be shared comprises:

- contact information held by various agencies on individuals who pose a high risk of harm to their partners or children
- personal information pertaining to high risk victims or their children

which will assist the MARAC to put in place safety measures to reduce/manage the risk posed.

b) This agreement relates to all personal and sensitive personal data about specific victims, alleged perpetrators and/or children of the household/s held by any partner agency that the

MARAC 'needs to know'[3] for the purpose of delivering safe and effective services to the victim at high risk of harm.

c) Personal data are: data relating to a living individual who can be identified from that data or any other information held or likely to be held. It also includes any expression of opinion about the individual and any indications of the intentions of any person in respect of the individual.

d) Sensitive personal data are: personal data consisting of information concerning racial or ethnic origin, political opinions, religious or other similar beliefs, trade union membership, physical/mental health or condition, sexual life, alleged or committed offences, proceedings, disposal or sentence concerning any alleged or committed offences (Information Commissioner's Office (2001)).

Does this include personal data under the Data Protection Act 1998?

a) Yes. The MARAC members will be sharing both *personal data* and *sensitive personal data* as defined in the Data Protection Act.

[3] The MARAC will be governed by appropriate procedures and partners will be provided with adequate training to recognise and deal with the issues of proportionality and necessity.

3. 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 (HRA)?
- Would there be a breach of a common law duty of confidentiality?
- Would there be a breach of the Data Protection Act 1998 (DPA)?

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 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.

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 measures 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 own statutory or other 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) The 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 working 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"*.

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.

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.[4]
- 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.[5]

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 in shared about individuals who pose a high risk of harm to their partners or children, or about high risk victims/victims and their children, then if the appropriate conditions in Schedule 2 or 3 are met, then 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. The Wandsworth MARAC referral form has an integrated 'Information Sharing Without Consent' form and this MUST be completed in all cases where consent has not been given. It is the responsibility of the referrer to identify which legal gateway/s they are using to share information and to indicate this on the form.

Data Protection Act 1998 (DPA)

The DPA 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 constitutes "processing" for the purposes of the Act. The eight principles are discussed below, in turn.

[4] Department for Constitutional Affairs (2003) Public Sector Data Sharing: Guidance on the Law. London: Department for Constitutional Affairs.
[5] Department of Health (2003) What to Do if You're Worried a Child is Being Abused. London: Department of Health.

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 victim 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 to the victim 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 victim, 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 victims) 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) Partners to the MARAC will put in place internal procedures to ensure that decisions to share personal information about the alleged perpetrator without his/her consent and without service of a fair processing notice will be appropriately recorded for audit purposes. These procedures are outlined in this Agreement in the *Description of Arrangements Including Security Matters*. 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 would be likely to increase risk to the victim 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 order[6] 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 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.

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.

[6] See SI 2000/417, Schedule, paragraph 1.

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 victim, 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, victims 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 victim, 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 (Wandsworth Community Safety Unit, Metropolitan Police) 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 in line with the Management of Police Information (MoPI) standards for the purposes of providing an audit trail. These records will be reviewed every ten years.

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 impose 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 victim and her/his children or is already providing services to or is involved in ongoing case work in respect of the victim, 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 victim and her/his children or who is already providing services to or is involved in ongoing case work in respect of the victim, 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 accessible to the individuals within the organisation who 'need to know' the information.

All signatories to this Agreement will keep information securely as set out in the Description of Arrangements Including Security Matters

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.

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 victims 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.

4. DISCLOSURE INTO COURT PROCEEDINGS

The Family Justice Council and CAADA have recently developed and published guidance on the disclosure of information into court proceedings *(Working Party of the Family Justice Council, December 2011).* This guidance states that

- The MARAC is not a legal entity and, therefore, the original supplying agency retains ownership of the information.
- MARAC's should only be required to supply information to the court by way of a court order.
- Any requests for information must be informed requests setting out the nature of the information sought.

Requests for disclosure should be made in good time to the MARAC chair who, if necessary, should raise any formal objection to disclosure. If no objection is raised the chair should identify which documents are held; if the information held was supplied by a partner agency, the court should be invited to request the information direct from that agency. This will apply to statutory and voluntary agencies.

5. DESCRIPTION OF ARRANGEMENTS INCLUDING SECURITY MATTERS

How the information will be processed

The information to be shared comprises contact information and personal and sensitive data held by various agencies on individuals who pose a high risk of harm to their partners or children, and personal and sensitive information pertaining to high risk victims/victims and their children, which will assist the MARAC to put in place safety measures to reduce/manage the risk posed.

The MARAC group will convene every four weeks to discuss high-risk cases and share information about the parties involved to allow action to be taken to manage the risk posed to the victim/victim and children, if present.

Currently the information will be shared between designated and named representatives from those agencies specified on page 4 of this agreement, and with other agencies identified as relevant by the MARAC Co-ordinator on a case-by-case basis including community based and voluntary perpetrator programmes, local drug and alcohol services, child and family support organisations.

At the start of each MARAC the Chair will read out the confidentially agreement that information discussed within the ambit of the meeting is strictly confidential and must not be disclosed to a third party without the agreement of the partners of the meeting. An attendance form, detailing this requirement and the purpose of the meeting, will be signed by all attendees confirming they agree to abide by these principles. All partners will ensure that their representatives in attendance will have been vetted to Criminal Records Bureau standard. Normally, in order to satisfy the Metropolitan Police Service protective marking security standards, further vetting of partner agencies' staff would be required. However, an exemption from further vetting is claimed under this agreement since all MARAC partners have a genuine "need to know".

Each domestic crime/incident recorded by the police is subjected to a risk assessment, firstly utilising the DASH model and, in medium and high risk cases, completion of a Part 2 Risk Assessment. A detective sergeant will supervise all risk assessments. Those identified, as being at high risk will be referred to the police MARAC co-ordinator for further referral to the Independent Domestic Violence Advocacy Service and MARAC. As agreed by the Wandsworth Borough MARAC Steering Group, referrals will be circulated to MARAC partners as and when they are received. The agenda will then be circulated to the MARAC group attendees eight days prior to the meeting to enable them to collate the information that they hold on the nominated parties that may assist in safety planning and risk management.

Other members of the MARAC group will also have the facility to refer high risk victims to the MARAC by use of the local bespoke referral form (compiled individually by each MARAC). All

referrals from partner agencies will be submitted to the MARAC via the agency's MARAC representative.

On receipt of such a referral the MARAC co-ordinator will add the details of the persons involved to the MARAC agenda and request other agencies to ascertain if they know the parties. All attendees will then be in a position to discuss the individuals and contribute to the safety planning.

The source of police information will be from a number of databases including: Police National Computer, CRIS, CrimInt, Merlin, 124D (domestic violence notebook) and Part 2 Risk Assessments. The information provided will be sufficient for partner agencies to interrogate their indices to establish if the parties are known to them, thus enabling them to provide further information to the MARAC group in order to provide a holistic view to the threat posed to the victim(s).

The MARAC co-ordinator will keep detailed records of all requests for information, detailing the agency requesting the information, the reason and necessity for the request, and the information provided. Where it has been decided that the release of the information is not appropriate this fact will also be recorded detailing the rationale for the refusal.

The MARAC Co-ordinator will retain all documentation relating to cases discussed which has informed the decisions taken by the MARAC in order to draw up the Action Plan for victims. The information retained will be subject to the Security arrangements set out in this Agreement and will provide an audit trail for decisions taken by the MARAC. Information not relevant to the MARAC will be securely destroyed.

Each agency will have a minimum of two contacts through whom the information and requests will be directed. Where the instance arises that no approved contact is available and information is being requested by another party, the MARAC co-ordinator will ascertain the necessity for providing this information and if there is a basis in law to do so. Where a basis in law exists the information will be conveyed to the third party and a record maintained of the transaction. The nominated persons for that organisation will also be made aware of the request and asked to review their list of nominated person to ensure sufficient cover is provided to facilitate the sharing of information in line with this protocol.

Training & Awareness

A programme of training and awareness will be developed and delivered to all MARAC participants to ensure they understand the protocols and procedures agreed. Various sources for training are available, ie CAADA, MARAC Chair's forums, CSU DI's conferences, etc and over time each MARAC will need to determine its own requirement for continuation training. Training should comprise elements of the following:

- Understanding risk in the context of domestic violence

- The role of the MARAC in reducing risk to victims of domestic violence
- Working in partnership – agencies' roles and responsibilities
- Case studies – routes to and through the MARAC
- Managing information legally and safely – why, when and how to share and store information

A copy of the information sharing agreement will be posted on the Metropolitan Police Service internet site and partners will be encouraged to do the same.

Security

Information will be shared via a secure email using the Government Secure Community (GSC) or CJSM service. Where the need to print off hard copies exists, there will be a minimum security requirement for all agencies to store the said information within a lockable cabinet within a room with a door that is locked and secured when the premises is vacant. Once paper copies have fulfilled their use they must be disposed of as confidential waste by shredding or other secure means. The Metropolitan Police Service will retain and review the material it has accumulated in line with Metropolitan Police Service procedures. Partner agencies will be encouraged to adopt a similar system.

Partners will have their own procedures for disposal of redundant electronic data.

Hard copies of information brought to the MARAC will be left in the meeting room. The MARAC will determine which documentation should be retained by the MARAC Co-ordinator in order to provide an audit trail for the decisions taken by the MARAC in respect of the Action Plan for victims. Any other material will be disposed of securely by the MARAC Co-ordinator immediately after the meeting.

Any security breaches will be reported to the Community Safety Unit (CSU) Detective Inspector, who will be responsible for disclosure to the MARAC Co-ordinator if non MPS staff fulfil that role. All agencies must have internal disciplinary policies in place for dealing with security breaches. Additionally, any security incidents or newly identified vulnerabilities will be reported to the CSU Detective Inspector and MARAC Co-ordinator. 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.

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.

The Metropolitan Police Service will retain all documentation relating to the MARAC for a minimum of ten years. The information will then be reviewed and a decision taken by the Community Safety Unit Detective Inspector as to whether the material should continue to be retained.

The MARAC chair will also periodically remind partner agencies at the MARAC meeting to ensure that their email accounts are being managed effectively, and seek assurances from the Team leaders that this is being done.

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.

Review

This document will be reviewed on a 12 monthly basis. The review will enable any amendments to be made and allow for additional signatories to be added should they be identified.

6. AGREEMENT

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners at least annually.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

Agency	Post Held	Name	Signature	Date

7. APPENDICES

Appendix 1: References

Home Office report 30

This report makes reference to the Home Office Development and Practice Report, Number 30, titled *"Safety and justice: sharing personal information in the context of domestic violence – an overview"* (2004), ISBN 1 84473 241 X

Home Office Development and Practice Reports are produced by the Research, Development and Statistics Directorate.

For further copies contact:
Communication Development Unit
Room 264,
Home Office,
50 Queen Anne's Gate, London
SW1H 9AT.

Tel: 020 7273 2084
Fax: 020 7222 0211
http://www.homeoffice.gov.uk/rds

Metropolitan Police Secure Email Guidance

Guidance: Options for use of secure email in support of purpose specific Information Sharing Agreements
Version 2.0; 25 December 2006
Information Sharing Support Unit (ISSU)
DoI 2(3) Public Access Office

Appendix 2: Confidentiality Statement

This is the confidentiality statement read out and signed at the beginning of each meeting

Wandsworth MARAC Confidentiality Statement

Date:

The chair of the meeting reminds all concerned of the protocols within the agreed MARAC Information Sharing Agreement. 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 the Information Sharing Agreement without the consent of the partners at the meeting. Information should focus on domestic violence 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, gender, sexuality and disability.

The purpose of the meeting is as follows:

⇨ To share information to increase the safety, health and wellbeing 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 jointly construct 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 victimisation.

⇨ To improve agency accountability.

⇨ To improve support for staff involved in high risk DV cases.

The responsibility to take appropriate actions rests with the individual agencies; it is not transferred to the MARAC. The role of the MARCA is to facilitate, monitor and evaluate effective information sharing to enable appropriate actions to be taken to increase public safety.

Appendix 3: Metropolitan Police Secure Email Guidance (version 1.0)

1. INTRODUCTION

1.1 GLOSSARY

These guidelines relate to various email systems and processes and the following is a glossary of the terms that are used:

Secure email	Any email solution that provides for the appropriate level of security (as accredited by the MPS Information Management and Security Section), for the transmission of information valued as RESTRICTED under the Protective Marking System (PMS).

BOCU	Borough Operational Command Unit
CJIT	Criminal Justice Information Technology
CJX	Criminal Justice Extranet
CJSM	Criminal Justice Secure email
GSC	Government Secure Community
GSI	Government Secure Intranet
GSX	Government Secure Extranet
NHS.NET	National Health Service Secure Extranet
PMS	Protective Marking System
PNN	Police National Network

1.2 BACKGROUND

The operational necessity for secure email links between the MPS and its key partners outside the service is apparent now and will increase. To support MPS staff in carrying out those policing duties that would be made more effective by secure email communications with partners for the transmission of **RESTRICTED** information; several approved options to achieve this have now been identified.

Please note that information valued as **NOT PROTECTIVELY MARKED** may be sent using normal email. Also, none of the options within this guidance is suitable for the transmission of information valued as **CONFIDENTIAL**. Few options exist for sending Confidential material but if necessary, further advice and clarification can be obtained by contacting the MPS Information Security Assurance Unit.

1.3 INFORMATION SHARING AGREEMENTS

This guidance will highlight the various options available, together with the applicability and the arrangements that must be in place for each. The technology featured in each of the options provides adequate security in the transmission of **RESTRICTED** information. However, clearly defined procedures to use any of the options is essential because the MPS must have assurances regarding the recipient's use of the information. Therefore, the use of any of the options should be part of an agreement developed, or if already in existence, reviewed using the corporate information sharing framework (SOP published in Notice 46/05). The "Process" section of the Purpose Specific Agreement allows for specific instructions to be clearly set out. This ensures that there is an accountable process that is easily understood by all those whose duty it is to carry out the sharing.

The Baseline Security Assessment stage (Stage 4) of the framework is concerned with all the aspects of security involving the sharing of any information but specifically suggests standards for the transmission of information electronically. This guidance gives the instructions on the detail that will mean that those standards can be met.

If any clarification or assistance is required with establishing any of the options set out here, contact the Information Sharing Support Unit for advice.

.

2. OPTIONS

2.1 OPTION A – EMAIL WITHIN THE GOVERNMENT SECURE COMMUNITY (GSC)

If the arrangement to share information is with a partner whose email addresses include the following extensions, **pnn, gsi, gsx, cjx**, this indicates that they are members of the Government Secure Community (e.g. @dfes.gsi.gov.uk or @london.probation.gsx.gov.uk). This means that a secure link between the MPS and the partner is already established. **Please note that the inclusion of gov.uk alone does not indicate membership of the GSC. Communications with partners whose email addresses only include this, such as local authorities, are not secure**. The use of email is rarely appropriate for operationally critical matters where immediate action is required. However, in the more usual partnership arrangements, a defined procedure setting out access to a "group mail box" (sometimes termed a "shared email box"), by a number of identified individuals should mean that matters will be dealt with effectively. Therefore as part of the arrangements to share information between the MPS and any other member of the GSC, the establishment of a group email box within AWARE and a similar arrangement by the partner, is the key step in ensuring the most effective process for managing the security of the information.

Clear local procedures must be prepared for all those involved in the activity that is to be supported by secure email. These will be tailored to the particular initiative or activity but issues such as

- Who will access the boxes?
- How often they must be accessed
- How it will be indicated that any particular message has been actioned and by whom?
- Where the information that is transmitted will be stored

are some that must be defined.

Exactly the same issues as above should be negotiated and agreed with the partner agency(ies) and both sets of procedures must be clearly shown in Stage 4 of the Purpose Specific Information Sharing Agreement, "Description of Arrangements Including Security Matters". If the partner is another police force, provided that the messages sent to them are clearly marked RESTRICTED, it can be confirmed with them at the start of the arrangement and included in any written agreement, that the force, like the MPS will comply with the handling rules for security prescribed by the PMS.

2.2 OPTION B – EMAIL WITH PARTNERS WHO ARE USERS OF CJIT (CJSM) SUCH AS LOCAL AUTHORITIES

CJSM is a Home Office supported programme that was developed to facilitate better communications between all those involved in the criminal justice system. However, the secure email facility provided as part of the programme, is one that can be used for many other purposes such as wider information sharing. The CJIT programme supports its wider application. Sending email between MPS .pnn email addresses and CJSM email addresses is as technically secure as Option A above. It means that those agencies that are not part of the GSC, for example Local Authorities or regulatory bodies such as the Security Industry Authority, can still have secure email connections with the members of the GSC and other CJSM users.

All London local authorities are now CJIT (CJSM) enabled. This is because all the Youth Offending Teams (YOTS) in London, which are included as part of local authorities' IT infrastructure, are now able to communicate securely with other criminal justice agencies. In any negotiations with London local authorities to develop or review information sharing agreements, at the outset it can be made clear that the MPS is ready to communicate with any as soon as they have configured their CJSM account appropriately and defined their procedures relating to the particular initiative. The MPS side of any partnership will then adopt the procedures already set out in Option A above**.**

2.3. OPTION C – EMAIL WITH THE NATIONAL HEALTH SERVICE

Although not officially a part of the GSC, partners that have **nhs.net** email addresses can send and receive emails with the MPS to the same level of security as the other options in this guidance. Technically, the system has been proved to be a secure transmission method but procedurally, issues still exist concerning its use. Our NHS partners have their own rules around the sending of patient related information even internally by email. At the time of writing this version of the

guidance, there is no common understanding between the NHS centrally and partners such as the MPS as to which information can be shared using this method.

However, as with our Local Authority partners and their use of CJSM, when the MPS is able to clearly demonstrate the benefits of a particular initiative, progress has been made with work involving the NHS. In particular, work being conducted on most BOCUs now on “BOCU Mental Disorder Referral and Case Conferencing” has led some boroughs to begin negotiating similar arrangements as set out in Option A above with partners from Community Mental Health Trusts. This work is ongoing but updates on progress will be included in later versions of this guidance. Any successful examples will of course inform future negotiations with all NHS partners.

DoI2 (3) Public Access Office
Information Sharing Support Unit
16.01.09