GREATER MANCHESTER
MULTI AGENCY RISK ASSESSMENT CONFERENCES

MULTI-AGENCY MARAC OPERATING PROTOCOL

V 0.5
September 2020
Public Protection Governance Unit

Version Record

Version No.	Amendments Made	Authorisation
0.1	First version for consultation with MARAC & Public Protection Training Co-ordinator	
0.2	Amendments made following consultation.	MARAC & Public Protection Training Coordinator Julie Church-Taylor.
0.3.3	Final version for signature	Public Protection Division Chief Superintendeny Paul Rumney.
0.4	Amendments made in relation to changes in Police operational practice	Public Protection & Serious Crime Division Public Protection Governance Unit Superintendent Gwyn Dodd

Summary of the main changes to Version 0.4 updated January 2020	
1.1.8	MCT (MARAC Coordinators Team) replaced with CMT (Case Management Team)
2.4	MARAC objectives updated in line with SafeLives guidance
2.5	Minor changes to the wording in line with SafeLives current guidance
2.7.3	Reference to specialists from the statutory and voluntary sectors
4.1.1	Changed to note that a fee is payable for SharePoint membership
4.1.2	Details of SharePoint lead for each area
4.1.3	Reference to individuals being bound by the MARAC Information Sharing Protocol and the MARAC Operating Protocol
4.1.5	MARAC Coordinators Team removed and GMCA substitued
4.5.15.4	Breakdown of the iOPS PoliceWorks DASH
4.5	Repeat referral definition updated in line with SafeLives guidance
4.14.3	Chairing arrangements amended
5.8	‘MARAC & Public Protection Training Coordinator’ replaced by ‘all MARAC agencies’.

Summary of the main changes to Version 0.5 updated September 2020	
General	Reformatted
1.	High risk definition updated to include the word “imminent”
1.2	Reference to the NPCC removed and substituted with “cross government”
1.5	Introduction to the ten principles updated to be in line with the SafeLives website
3.4	References to MARAC as the forum for DVDS removed
4.3	“National Probation Service and Community Rehabilitation Company” replaced with “Probation services”
5.3	Process replaced with SafeLives recommended process
5.4	Clause following this removed (reference to the MARAC being the DVDS forum)
9	Reference to the meeting being Chaired by GMP removed and amended to reflect flexibility across the ten local authority areas
Appendix 2	Flowcharts amended to reflect changes at 5.3

1. TERMS AND DEFINITIONS

1.1. Acronyms

In this document the following acronyms shall have the following meanings:

GMCA	Greater Manchester Combined Authority
GMP	Greater Manchester Police
High Risk	An imminent risk that is life threatening and/or traumatic and from which recovery, whether physical or psychological, can be expected to be difficult or impossible.
IDVA	Independent Domestic Violence Adviser
MARAC	Multi Agency Risk Assessment Conference
MOP	MARAC Operating Protocol
NPCC	National Police Chiefs' Council
Partner Agencies	Agencies with MARAC SharePoint membership who participate in the MARAC process
Receiving area	an area where a MARAC referral is forwarded to in those cases where a victim relocates
SafeLives	A national charity, founded in 2005, dedicated to ending domestic abuse who assisted in the establishment of the use of the SafeLives DASH Risk Identification Checklist and who were commissioned by the Home Office to set up the MARAC meetings in England and Wales. SafeLives are considered to be the arbiters of best practice for MARAC in England and Wales.
SharePoint	Secure workgroup hosted on the GMCA server

1.2. Domestic Abuse Definition

The MARAC has adopted the NPCC definition of domestic abuse as any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality. This can encompass, but is not limited to, the following types of abuse:

- Psychological
- Physical
- Sexual
- Financial
- Emotional

Controlling behaviour is: a range of acts designed to make a person subordinate and/or dependent by isolating them from sources of support, exploiting their resources and capacities for personal gain, depriving them of the means needed for independence, resistance and escape and regulating their everyday behaviour.

Coercive behaviour is: an act or a pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim.

In addition this definition incorporates issues such as forced marriage, female genital mutilation and so called 'honour' based violence, as well as elder abuse when committed within the family or by an intimate partner.

Family members are defined as mother, father, son, daughter, brother, sister and grandparents, in-laws and step-family.

1.3. MARAC

The MARAC is a Multi-Agency Risk Assessment Conference for the highest risk victims of domestic abuse.

Cases featuring forced marriage, female genital mutilation or so called 'honour' based violence should always be considered to be high risk and referred to MARAC where it is safe to do so. Please see clause 5 of this Protocol for further information.

In a single meeting, MARAC combines up to date risk information with a timely assessment of a victim's needs and links those directly to the provision of appropriate services for all those involved in a domestic abuse case: victim, children and perpetrator.

1.4. MARAC objectives

- To safeguard victims of domestic abuse
- To manage perpetrators' behaviour
- To safeguard professionals
- To make links with all other safeguarding processes

1.5 The ten principles of an effective MARAC

The four aims of MARAC are to safeguard victims of domestic abuse, manage perpetrators' behaviour, safeguard professionals and make links with all other safeguarding processes.

The ten principles underpin an effective MARAC and support everyone involved to deliver these aims. At the core of each principle is the safety of the victim, which needs to be considered at all stages of the process. Ensuring that the victim is supported throughout and their needs represented at the MARAC is crucial to managing risk, improving and maintaining safety, and reducing repeat victimisation.

Identification	Professionals recognise domestic abuse, risk assess and identify high-risk cases based on the referral criteria for MARAC
Referral to MARAC and IDVA	All victims who meet the MARAC threshold are referred to MARAC and IDVA
Multi-agency engagement	Agencies that can contribute to safeguarding high-risk victims, associated children and vulnerable adults attend the MARAC
Independent representation and support for victims	All high-risk victims are offered the support of an IDVA; their views and needs are represented at MARAC

Information sharing	MARAC representatives share relevant, proportionate, risk-focused information
Action planning	Multi-agency action plans address the risk to the victim, safeguard children and adults at risk, and manage perpetrator behaviour
Number of cases	The MARAC hears the recommended volume of cases
Equality	The MARAC addresses the unique needs of victims with protected characteristics
Operational support	There is sufficient support and resource to support effective functioning of the MARAC
Governance	There is effective strategic support and leadership of the MARAC and IDVA response, and agencies work together effectively

1.5. **Purpose of Protocol**

The purpose of the MOP is to establish accountability, responsibility and reporting structures for MARAC and to outline the process of the MARAC.

1.6. **Agency accountability and responsibility**

MARAC has a core membership comprising the responsible strategic leads from the statutory and voluntary sector agencies that work directly with victims and offenders. In addition, some agencies may attend as required, should they refer a case in or should a case have particular relevance to their service.

Any agency making a referral to MARAC must attend the meeting at which the case is to be heard.

Core MARAC agencies who should be in attendance at every meeting are:

- Police
- IDVA Service
- Housing
- Children's Social Care
- Probation services
- Health
- Mental Health
- Substance Misuse
- Adult Social Care

Ideally there should also be representation from other specialists from the statutory and voluntary sectors.

The MARAC can only operate effectively if all member agencies participate fully in the process. This means in addition to attending the MARAC meeting, they must also ensure that effective systems are in place within member organisations to meet the requirements of the MARAC.

The purpose of the MARAC is to reduce the risk of further abuse to those victims of domestic violence who have been assessed as at high risk of such abuse. This is achieved through sharing information between agencies, to ensure that a full picture of the risk can be identified and appropriate measures implemented to reduce the risk.

In addition the aim is to ensure that whichever agency a victim meets or discloses to, they receive an appropriate response that reflects their experience of domestic abuse. Where possible agencies should offer support so that cases do not escalate to high risk, at a minimum this should result in referral or signposting to the appropriate specialist support.

Member agencies should ensure that:

- Relevant staff and managers have received Domestic Abuse Training.
- Front line staff, working with individuals / families, and their managers, have also received training on the DASH Risk Assessment model and MARAC process.
- Staff are confident to assess risk, understand the local risk thresholds, and refer high risk cases to the MARAC
- Referrals to MARAC are of good quality e.g. all relevant information is clearly provided
- They have a process for ensuring risk assessments are carried out
- There must be a process for internal quality assurance (e.g. a MARAC champion role identified) to ensure that referrals into the MARAC are high risk and that the referral form and DASH Risk Identification Checklist have been properly completed with all relevant information. In particular, the reason for the referral should be clear and for those cases referred in on the basis of Professional Judgement a full rationale for the referral must be given
- Once a case has been assessed as high risk by any agency and confirmed by the MARAC Champion, all members work together to address the risk both before and after the MARAC meeting.
- A named individual is the regular representative for the MARAC, and is of the level of seniority that can suggest/agree actions for their agency and take responsibility for ensuring that actions are carried out, and information is passed back to the worker dealing with the case.
- A named deputy will attend the MARAC in that person's absence.
- Upon publication of the of the MARAC Agenda to SharePoint the agency will ensure that research form is completed for all cases known to the agency, and the information passed to the MARAC representative.
- At the MARAC representatives will suggest actions to reduce risk.
- After the MARAC representatives will ensure that agreed actions are carried out to the required timescale
- MARAC cases are flagged/marked on all agencies systems, to show that the individual has previously been referred to the MARAC.
- Staff are aware of what a MARAC flag or marker means and take this into account during any future contact work

The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC.

The role of the MARAC is to facilitate, monitor and evaluate effective information sharing to enable appropriate actions to be taken to increase public safety.

2. GOVERNANCE AND PERFORMANCE MANAGEMENT

Partner Agencies will support the objectives of the MARAC at clause 1.4 of this protocol.

2.1. MARAC Steering Group

The MARAC should be governed by a local MARAC Steering Group that meets four times a year.

A local MARAC Steering Group may be part of a larger multi-agency strategic group. The core responsibilities of a local MARAC Steering Group are: -

- To operate in accordance with its Terms of Reference;
- To monitor and evaluate the data from the MARAC;
- To ensure appropriate strategic links with the MAPPA are maintained;
- To ensure that effective partnerships are maintained with other public protection bodies and other MARAC areas;
- To monitor and regularly assess in accordance with the SafeLives self-assessment quality assurance process the overall performance of the MARAC and ensure it operates in line with the 10 Principles of an effective MARAC referred to at clause 1.5;
- To address any operational issues;
- To report to the local strategic partnership;
- To oversee efforts to raise awareness with local practitioners about the MARAC;
- To communicate the performance of the MARAC to key stakeholders;
- To ensure that the MARAC is compliant with legal responsibilities and keeps up to date with changes to legislation national guidance;
- To participate in reviews following a homicide where appropriate.

2.2. Data Collection

- GMP staff will collate MARAC data in accordance with SafeLives Guidelines.
- Unborn children will not be included in the MARAC data as children.
- De-personalised data is available on request from GMP's Domestic Abuse Coordinator.
- Depersonalised information is shared with central government when required.
- Depersonalised standard data is available to MARAC agencies on request from GMP's Domestic Abuse Coordinator
- When requesting data from the GMP Partner Agencies are requested to give seven days' notice
- If a victim as aged 16 or 17 he or she will not also be counted as children for statistical purposes

3. PROCESS OF THE MARAC

3.1. SharePoint

The MARAC is administered via a SharePoint application that is a secure workgroup on the GMCA website. The workgroup is only visible to designated individuals in partner agencies who have been granted access.

All MARAC documentation is shared via SharePoint and by no other means.

SharePoint membership is subject to a fee and is granted by the local authority Domestic Abuse lead for each individual area

Individuals who are granted SharePoint membership are bound by both the Greater Manchester MARAC Information Sharing Agreement and MARAC Operating Protocol.

There is a requirement for each individual SharePoint member to add their full contact details to the site. Failure to do so will result in membership being suspended.

SharePoint access is regularly reviewed by GMCA and any individuals not using the site will have their individual SharePoint memberships suspended.

SharePoint log-ons must not be shared. If a partner agency requires additional log-ons these should be requested by email to the relevant SharePoint Area Lead

If an individual is leaving his or her workstation whilst logged in to the SharePoint site the computer screen should be locked

MARAC referrals should be on the prescribed local form copies of which are available on the relevant SharePoint sites

Partner Agencies will upload their referral forms to SharePoint; referrals cannot be accepted by email or any other means.

The Referral Form should be uploaded within 24 hours of the trigger incident or an agency becoming aware that a victim is at a high and imminent risk to enable partner agencies to commence research and for the IDVA service to make pre-MARAC contact with the victim.

All referrals must be uploaded in Microsoft Word format.

Scanned and handwritten referral forms are not accepted.

If a partner agency is unable to complete an action previously volunteered at MARAC, they will advise other agencies by way of an announcement on SharePoint and report the failure/inability to complete to the Chair at the next MARAC meeting.

MARAC documentation will not be exchanged by any method other than by being made available on the SharePoint site.

All MARAC documentation will be available from SharePoint.

Completed MARAC documentation should not be printed unless strictly necessary due to the sensitive and confidential nature of the information contained in the documents.

3.2. Quality Assurance Requirements for MARAC referrals

MARAC referrals should be named as name of victim and referral date [SURNAME Forename 060816]. This enables the building of a uniform database on SharePoint.

Referral forms should be fully completed. If any information is not available or not applicable, this should be clearly marked on the form.

When a case has been referred on the criterion of Professional Judgement a rationale for that judgement must be given.

DASH Risk Identification Checklists should contain brief detail in the comments boxes provided.

The referring agency must check Referral Forms to ensure they are complete. It should be noted that failure to submit a properly completed referral could compromise the safety of a victim and his or her children.

If amendments are required to a referral form once it has been uploaded, the GMP staff with responsibility for MARAC should be notified and will arrange for any necessary amendments by striking through the original text, adding the new text in red and placing an announcement on the relevant part of the SharePoint site stating amendments have been made.

3.3. General

The MARAC operates on the basis agencies that need to be involved with a case already are and that normal partnership working practices are in place.

Partner agencies should not wait for the MARAC meeting to commence any work with the victim.

3.4. Domestic Violence Disclosure Scheme (DVDS)

All information shared at MARAC should be considered for disclosure to the person at risk under the DVDS Right to Know.

4. Screening and Risk Assessment

In order for a MARAC process to work effectively there needs to be a common understanding of risk among the participants.

Risk Indication: the process of gathering information on the prevalence of academically researched risk factors or risk indicators

Risk Assessment: the process of analysing and grading the information received around risk indication

Risk Management: the management (normally based on the risk assessment grade) of a case either on a single agency basis or multi-agency basis. Risk Assessment informs the risk management process.

Risk factors / Risk indicators: the variables that are be used to assess the likelihood of further harm.

Harm: the amount and type of harmful behaviour being indicated.

Risk: the likelihood or probability that harm will occur. This is an estimate that will change overtime and context.

Clinical Assessment: The clinical assessment of dangerousness is based on an individual practitioner's judgement of a situation.

Actuarial Assessment: This involves a numerical grading approach and the prevalence of risk factors to compute the probability of harms occurring (NPCC/SafeLives DASH).

SARA: The SARA tool used in the Prison and Probation services is an international validated aid to the assessment of risk of harm in domestic abuse cases.

Greater Manchester Police Risk Assessment of Victims: Risk assessment comprises the middle section of a three stage domestic abuse response formed around Risk Indication, Risk Assessment and Risk Management. Once a domestic abuse issue has been identified or a report received a risk assessment assesses the likelihood or probability of the risk of further harm occurring to that person. The purpose of a risk assessment is to inform a risk management plan that will try to reduce the likelihood of further incidents happening.

4.1. **Risk Grade Definitions**

- Standard: no significant current indicators of risk of harm.
- Medium: there are identifiable indicators of risk of harm. The offender has the potential to cause harm but is unlikely to do so unless there is a change in circumstances, for example, failure to take medication, loss of accommodation, relationship breakdown, drug or alcohol misuse.
- High: there are identifiable indicators of risk of serious harm. The potential event could happen at any time and the impact would be serious. The Oasys definition is "a risk that is life-threatening and/or traumatic and from which recovery, whether physical or psychological, can be expected to be difficult or impossible".

4.2. **Risk Factors or Risk Indicators**

Risk factors can generally be divided into 5 main categories:

1. Nature of the abuse e.g. emotional, physical, sexual
2. Historical patterns of behaviour e.g. previous convictions or abusive behaviour
3. Victim's perception of risk e.g. specific fears for themselves and children, pets
4. Specific factors associated with an incident e.g. use of weapon, threats to kill
5. Aggravating factors e.g. drugs, alcohol, financial problems

Factors can also be separated out between Victims circumstances and Offenders behaviours/circumstances.

4.3. **Developing a Common Understanding of Risk**

It is important for the MARAC process that all members share a common understanding on risk thresholds and levels of risk. This is achieved by adopting standardised risk indication and risk assessment tools.

Referrals to the MARAC from all agencies other than the Police and Probation services are based on the SafeLives DASH identification Checklist process. In order to achieve the commonality of approach outlined above it is recommended that if at all possible all referrals are based on the SafeLives methodology.

Probation services referrals will be based on the level of risk posed by the Perpetrator based on the SARA.

Police referrals are submitted on the criterion of professional judgement based on an assessment of the NPCC DASH responses and information around the threat posed by the perpetrator from Police systems when available.

4.4. **Risk Management**

In general cases which are submitted to a MARAC are submitted because of the degree of risk a victim may be exposed to and the fact that actions based on single agency information and single agency risk management are unlikely to be effective in keeping an individual safe.

To ensure that such cases are managed effectively they require multi-agency information sharing alongside multi-agency risk management. Most of the actions that arise from the MARAC reflect an altered perception of risk as a result of the information shared and therefore a more tailored response for the victim. With additional information, agencies are more able to prioritise actions, to support the victim and to support their staff.

To assist in this process:

- All agencies will routinely screen for domestic abuse.
- Where domestic abuse is present agency staff will use their best endeavours to assess the risk by use of the SafeLives DASH Risk Identification Checklist that forms Appendix 1 of this document where possible within two working days of an initial disclosure of domestic abuse.
- GMP use the iOPS PoliceWorks DASH which comprises the original NPCC 27 questions, the 11 stalking and harassment questions (where appropriate), the HBA questions
- A breakdown of the iOPS PoliceWorks DASH appears below:

IOPS DASH	Notes
1-7	Questions about the current situation, numbered exactly as in the NPCC 1-27
8	Trigger question to open up the SDASH (stalking DASH). This is question numbered 8 in the NPCC 1-27

9-19	SDASH questions, not previously available in OPUS
20	Trigger question to open up the standard DASH questions for children. This question is supplemental to the 1-27
21-24	Questions around children previously numbered 9-12 in the 1-27
25-31	Domestic violence history, previously numbered 13-19 in 1-27
32	Trigger question to open up the Honour Based Abuse DASH questions. Previously question 20 in the 1-27
33-42	HBA questions, not previously available in OPUS
43-49	21-27 in the 1-27
50	28 in the 1-27
51-55	New guidance for officer input

4.5. **Framework to Manage Risk**

All of the information provided by the risk indication and risk assessment elements of the process will have identified the issues and risk factors / indicators which underlie each case. These specific areas of concern now need to be managed in order to reduce risk. To achieve the necessary protection it is useful to have a framework around which management objectives can be set.

One such framework is RARA, used by Greater Manchester Police. RARA is a simple mnemonic which outlines four categories of case that can be impacted on by different types of management intervention. They include cases in which it is possible to remove the risk to the victim, avoid the risk to the victim, reduce the risk to the victim and cases in which there has to be some acceptance of risk to the victim because of insurmountable difficulties (at any given point in time) in achieving more positive intervention. See below for an outline of RARA and intervention examples:

- Remove the risk: By arresting the suspect and obtaining a remand in custody (short term only)
- Avoid the risk: By re-housing victim / significant witnesses or placement in refuge / shelter in a location unknown to suspect or sanctuary scheme.
- Reduce the risk: By joint intervention / victim safety planning, target hardening and use of protective legislation or re-house the perpetrator. Use of Domestic Violence Protection Orders.
- Accept the risk: By continued reference to the Risk Management Model (MARAC or MAPPA), continual multi-agency intervention planning, support and consent of the victim (via IDVA) and by pro-active offender assessment and offender targeting.

5. Referrals

All partner agencies must be aware of the threshold for proportionate and legal information sharing.

In cases where domestic abuse has been disclosed and there has been a recent incident (within 30 days) or there is an immediate risk of serious harm to the victim, the threshold for referral will be: -

- Visible High risk – 14 or more 'yes' responses on the SafeLives DASH Risk Indicator Checklist.
- Potential Escalation – The number of police callouts to the victim as a result of domestic abuse. This can be used to identify cases where there is not a positive indicator of a majority of risk factors on the list, but where the abuse appears to be escalating and where it is appropriate to assess the situation more fully by sharing information at the MARAC.
- Professional judgement – If a professional has serious concerns about a victim's situation, they should refer the case to MARAC. There will be occasions where the particular context of a case gives rise to serious concerns even if the victim has been unable to disclose the information that might highlight their risk more clearly. This could reflect extreme levels of fear, cultural barriers to disclosure, immigration issues or language barriers, particularly in the case of honour-based violence. This professional judgement would be based on the professional's experience
- Repeat victimisation as defined in clause 5.1 of this Protocol.

Forced Marriage[1] and so called "honour" based violence[2] should always be considered as high risk in a domestic setting and should be referred to MARAC unless there are specific

[1] Forced marriage is a form of domestic abuse and where the person is under 18 years old constitutes child abuse.

"A marriage conducted without the valid consent of one or both parties, where duress is a factor".

In **arranged marriages** the families of both parties take a leading role in arranging the marriage but the choice as to whether or not to accept the arrangement remains with the prospective spouses.

In **forced marriages**, one or both spouses do not (or, in the case of some vulnerable adults cannot) consent to the marriage and some element of duress is involved. Duress can include physical, psychological sexual and emotional pressure from the family and community and fear of bringing shame on the family if they refuse.

Forced marriage is a violation of internationally recognised human rights and cannot be justified on any religious or cultural basis. Parents who force their children to marry often justify their behaviour as protecting their children, building stronger families and preserving cultural or religious traditions. They do not see anything wrong in their actions. Forced marriage is not a religious issue: every major faith condemns it.

Although there is no specific offence of 'honour' based violence or forcing someone to marry within England and Wales, criminal offences may nevertheless be committed. Perpetrators, usually parents or family members could be prosecuted for offences including conspiracy, threatening behaviour, assault, kidnap, abduction, theft of the individuals personal belongings (often official documents such as a passport), threats to kill, imprisonment and murder. Sexual intercourse without consent is rape, regardless of whether this occurs within a marriage or not. A person who is forced into marriage is likely to be raped and may be raped until she becomes pregnant.

For many individuals, turning to the police is a last resort. Many may not even discuss their worries with a friend for fear of being found out by their family.

Whilst victims of a forced marriage are generally women, young men may also be at risk. Often the issue around forced marriage and a victim's reluctance to engage with it can lead to them suffering 'honour' based violence. The risks to the victim cannot be underestimated and past cases where the family have become aware that a victim has disclosed outside the family have resulted in severe beatings, dowry abuse, house arrest and even murder.

To avoid the serious consequences that can result from losing one's honour, individuals, families and communities may take drastic steps to preserve, protect or avenge their 'honour'.

In some cases people may be taken abroad without knowing that they are to be married. When they arrive in the country their passports and possessions may be taken from them to stop them returning home. In these circumstances they often don't know where to go for help and it is vital that we ensure that potential victims know what to do and where to turn to if they are out of the country and a marriage is forced upon them.

sensitivities around the case that cannot or should not be shared with a wider audience and that are instead better managed by taking a multi-agency Operation Challenger approach.

5.1 Repeat referrals

SafeLives defines a 'repeat' as ANY instance of abuse between the same victim and perpetrator(s), within 12 months of the last referral to MARAC.

The individual act of abuse does not need to be 'criminal', violent or threatening but should be viewed within the context of a pattern of coercive and controlling behaviour.
Some events that might be considered a 'repeat' incident may include, but are not limited to:

- Unwanted direct or indirect contact from the perpetrator and/or their friends or family
- A breach of police or court bail conditions
- A breach of any civil court order between the victim and perpetrator
- Any dispute between the victim and perpetrator(s) including over child contact, property, divorce/ separation proceedings etc.

These events could be disclosed to any service or agency including, but not exclusive to, health care practitioners (including mental health), domestic abuse specialists, police, substance misuse services, housing providers etc.

Where a repeat victim is identified by any MARAC agency, that agency should refer the case back to the MARAC, regardless of whether the behaviour experienced by the victim meets the local referral threshold of visible high risk, escalation or professional judgement.

To identify repeat victims of domestic abuse regardless of to whom it is reported, all MARAC agencies should have the capacity to 'flag and tag' their files following the latest referral so that they are aware if a service user experiences a repeat incident.

Incidents that occur more than 12 months after the date of the last MARAC referral within the same local authority area do not constitute a repeat incident but should be referred back to the MARAC.

Many cases involve the victim being married abroad and being brought back into the United Kingdom. Often these victims are freely entering into what they believe is an arranged marriage unaware that their partner is marrying under duress. It is not until the victim arrives into the country that the abuse begins and that they become aware of what has happened. Many of these victims will not have the confidence or know how to report the incidents to the police. Often these individuals do not have recourse to public funds.

2 'Honour' Based Violence is a form of domestic abuse. In the definition of domestic abuse family members are defined as mother, father, son, daughter, brother, sister and grandparents whether directly related, in-laws or step family. However with cases of HBV it is known that extended family members and members of the community can be involved who support the family's actions or collude in or perpetrate the violence on behalf of the family. You should never underestimate the level of involvement they may have in the violence.

'Murders in the name of so called 'honour'' are murders where victims are killed for their perceived immoral behaviour, which is deemed to have breached the 'honour' code of a family or community causing shame. There is however no 'honour in murder'. (ACPO 2006)

Such murders occur where, most often wives are killed by their husbands and daughters by their fathers. Males can also be victims, sometimes as a consequence of their involvement in what is deemed to be an inappropriate relationship, e.g. if they are gay, or if they are believed to be supporting the victim.

Relatives, both male and females, may conspire, aid, abet or participate in the killing. Younger relatives may be selected to undertake the killing, to avoid senior family members being arrested. Sometimes contract killers are employed. A decision to kill may be preceded by a family council. There often tends to be a degree of premeditation, family conspiracy and a belief that the victim deserves to die.

Repeat incidents as defined above should be noted on both the referral form and SharePoint.

GMP staff will record repeat incidents using the SafeLives MARAC Data Form.

The definition of repeat incidents above does not include cases that are being referred for a second time for any other reason than where there has been a repeat incident. There are specific instances where a further referral might be made but no repeat incident has occurred, such as, for example, where a perpetrator is about to be released from jail, where potential risks are identified but no specific threats have been made and the case is discussed in order to make sure that every agency is aware and able to put in place any appropriate safety measures.

5.2 Uploading referrals

Cases are referred to the Greater Manchester MARACs by uploading the relevant MARAC Referral Form onto SharePoint. Copies of the form are available on SharePoint.

All required details should be given on the Referral Form. If information is not available or a victim is unwilling to disclose certain information, this should be noted on the referral form rather than leaving the information box blank.

Number of children in the household is defined as:

- A child is defined as anyone age 17 or under who is not themselves referred as a victim or a young person causing harm.
- Children from both new and repeat cases should be counted in this column.
- If a woman is pregnant, the unborn baby does not count as a child.
- If the victim is aged 16 or 17, a decision will need to be made whether the case should be referred as a child protection case, or whether it should be referred to MARAC.
- The number of children in the household is counted as the number of children normally expected to be in the house on a regular basis and who would therefore be affected by domestic abuse.
- Those in long term care would be excluded, and short term included.
- Do not record anyone aged 17 or below who is the victim or person causing harm under the heading ‘Number of children in the household’.

All partner agencies can refer cases to MARAC.

The deadline for referrals is eight working days prior to the MARAC and this is noted on SharePoint.

The date of the next available MARAC appears on SharePoint during the upload process.

5.3 MARAC to MARAC referral process

This was developed by SafeLives to ensure there is clear guidance on the transfer of cases between MARACs when high risk victims move from one area to another, after a need for a

safe and consistent approach was identified. The aim is to promote the safety of high-risk victims, regardless of where they live, and to ensure that all agencies at MARAC are clear about their roles and responsibilities at each stage of the transfer process. The procedure has a number of key assumptions:

- That where a victim moves between areas, the MARAC agencies in the new area should notified;
- That the procedure should promote a consistent, victim focused response to the transfer of cases across MARAC areas;
- That a referral to a new MARAC should not be contingent on that victim meeting the local MARAC threshold in the area to which they are referred; and
- That the originating and receiving MARAC should have clear responsibilities at both the point of referral and in the 12 months since last referral (i.e. 'flagging and tagging' for further incidents')

The process is for both transferring cases out and receiving cases in. The transfer process is set out in the flowchart forming Appendix 2 hereof.

5.4 Duplicate referrals

Agencies should check SharePoint before uploading a referral to MARAC. If another agency has already uploaded a referral for the same case at the same MARAC the referral document name should be amended so that the word "DUPLICATE" appears at the end.

6. MARAC Agenda

The MARAC Agenda will normally be posted to SharePoint seven working days prior to the date of the MARAC and no other notification will be issued.

Amended/updated Agendas may be uploaded. These will be version controlled and an announcement will be put onto SharePoint to advise. Partner agencies should check to ensure they are using the most recent version of the Agenda.

Repeat cases will be listed at the beginning of the Agenda.

The MARAC allocates ten minutes to each case depending and the timings will be shown on the Agenda.

7. Actions before the MARAC

Agencies should consider the risk to the victim and take any actions for immediate safeguarding as may be necessary.

In every instance the agency submitting the case should implement a single agency risk management plan to take whatever steps possible to ensure victim safety. They should not delay actions by waiting for the case to be heard at the MARAC.

In cases not reported to police (if the victim is willing) a police intervention should also be initiated.

In cases where there are children or vulnerable adults involved, Social Services may also take some immediate precautionary measures ahead of the meeting.

It is the referring agency's responsibility to inform the victim (in a safe manner) that their case will be discussed at a MARAC.
Consent for the case to be referred to MARAC must be sought from the victim but lack of such consent should not prevent the case from being referred to the MARAC.

Agencies are required to research each case prior to the MARAC.

It is the role of representatives at MARAC to bring any information about the alleged perpetrator's circumstances and their behaviour for every case, as well as information about the victim and any children.

Where children, unborn children or vulnerable adults are identified within a MARAC case then a safeguarding referral should be made in line with the policy of each individual agency. Those referrals should be made immediately without waiting for the MARAC to take place.

All agencies are required to flag and tag files that are scheduled to present at MARAC.

Any help or advice offered by an Agency in connection with a particular referral should be started or continued before the MARAC.

8. Victim contact before the meeting

The IDVA service checks SharePoint daily for new referrals and in cases where consent for information sharing has been given, the IDVA service will endeavour to contact the victim prior to the MARAC in order to obtain the views of the victim for presentation to the MARAC and to offer immediate support with safety planning.

In cases where consent for information sharing has been given then in most cases the IDVA service will notify the victim of the MARAC and feed back to the victim following the MARAC unless alternative arrangements are agreed and captured as a separate action at the meeting.

If consent for the referral to the MARAC has not been given it will be at the discretion of the relevant IDVA service whether or not to contact the victim prior to the meeting.

9. MARAC meetings

The dates and times of the MARAC meetings are published to SharePoint.

The venue for the MARAC meeting is as noted on SharePoint.

The MARAC is chaired in line with other local arrangements.

9.1 The role of the Chair

To read out the confidentiality statement at the commencement of each meeting and to ensure that all persons present sign the statement.

To review any actions that may be outstanding from the previous meeting and to ensure that they are clearly noted in the audio recording.

To structure the meetings and prioritise cases in such a way that all those attending are able to use the time available as efficiently as possible.

To ensure the meeting runs in accordance with the timings shown on the Agenda.
To ensure that all information relevant to the perpetrator and factors that are likely to increase the risk of re-abuse to the victim, harm to children, other vulnerable parties and risk that agency staff could be harmed, is heard at the meeting. This would be in addition to the usual proportionate and relevant information shared on the victim and any children.

To outline the risks identified from all the information shared and to invite other representatives to highlight any additional concerns that may have been overlooked.

To ensure that actions volunteered by agencies are SMART (specific, measurable, achievable, realistic and timely).

To ensure that agency representatives understand actions and timescales they have volunteered.

To identify the specific risk that each action relates to.

To ensure that equality and diversity issues are considered in each case.

To state whether or not the case has the victim's consent for the MARAC referral.

9.2. **Public Protection**

Multi Agency Public Protection Arrangements (MAPPA) supports the identification, assessment and management of relevant sexual, violent and other dangerous offenders.

The aim of MAPPA is to ensure that a robust risk management plan is developed by the lead agency by working with other agencies involved with MAPPA through information sharing, focusing resources and putting measures in place which are coordinated through MAPPA to enable the agencies involved in MAPPA to protect the public.

MAPPA were introduced in 2001 and bring together the Police, Probation Services and Prison Service into what is known as the MAPPA Responsible Authority.

Other agencies are under a duty to co-operate with the MAPPA Responsible Authority including social care services, health, housing and education services.

Where a Partner agency is managing an offender under MAPPA Level 1 and becomes aware of an increased risk to the victim, that agency should make a referral to MARAC in the usual way.

The fact that the offender is under MAPPA should be disclosed to the MARAC as part of the information shared by the introducing agency.

If the referring agency is not Probation services, a Probation services representative at the MARAC meeting should take an action to feed back to the Offender Manager involved in the case under MAPPA that the offender has been the subject of a MARAC.

Where the police or Probation services are actively managing the offender, but not at MAPPA level 2 or 3, they will use the information provided by the MARAC to reassess the level of risk the offender presents to assist them in the effective management of the case. This could lead to the offender being referred to a level 2 or 3 MAPP meeting.

Where such a is made in accordance with the above, the IDVA service will be invited to the MAPP meeting (as well as any other professional who has relevant information) to ensure that information about the victim and their views are discussed and to ensure that the safety of the victim is central to the process. This will support the effective management of the offender and reduce the potential risk of harm to the victim.

Many MARAC cases do not result in a court appearance. Where criminal proceedings are pending, a MARAC is likely to take place before the case reaches a conclusion, which means that there is no conviction for the most recent offence. The perpetrator may have previous convictions and may be under current management because of their offending by the police and/or the Probation services and this can include MAPPA management at level 2 or 3.

Where an offender is already being managed at MAPPA level 2 or 3, to avoid duplication of effort and resources, it is best practice to hold one meeting and this should be the MAPP meeting.
MAPPA cases should not subsequently be referred to a MARAC. The MARAC has no statutory obligations to risk manage MAPPA category offenders. As stated in the introduction “the responsibility to take appropriate actions rests with individual agencies” and the statutory responsibilities around MAPPA are not transferable to a MARAC.

If, due to geographical or personnel constraints, this is not feasible, the two Chairs should liaise regarding planned actions to avoid conflicting Risk Management Plans being put in place.

9.3 **Presentation of information**

The MARAC allocates ten minutes for each case to be discussed at MARAC. This includes presentation of the case, sharing of the information, identification of the risks, action planning and consideration of equality and diversity issues.

The Agency that has referred the case should present it at the MARAC.

If a case has been referred in by a different Greater Manchester Police District then the Police will be asked to present the case. If the case has been referred in by any other non-local agency then the IDVA service will be asked to present the case as they will normally have had contact with the victim prior to the MARAC.

Agency representatives should state their name and agency each time they speak so that the origins of information are clearly identified on the audio recording.

The presentation should include brief details of the incident or immediate risk that has prompted the referral together with any other information in accordance with clause 4.17 of this MOP.

Following the presentation of information by the referring Agency representative, the Chair will then invite each Agency representative in turn to share any additional relevant information they hold and identify any further risks of which they are aware.

Agency representatives are required to clarify what is fact and what is opinion.

If an Agency representative is unable to attend it is required that a deputy representative attend instead.

If any Agency is holding information that has already been shared at the meeting then there is no necessity to repeat the information.

GMP does not accept research from agencies who choose not to attend a MARAC meeting.

9.4 **Inappropriate Referrals**

There may be referrals that, based on the information in the referral, may not appear to be high risk. MARAC is an information sharing process so it may well be that part of the information shared will identify that the risk is high.

If a case has been referred with consent, then there is no issue hearing it. The Chair will summarise the current risk when all the information has been shared. If it is the consensus of all MARAC partners present that the case is not a high risk case then it is crucial it is identified as such.

It is very important that offenders who are not high risk perpetrators and victims who are not high risk victims are not labelled as such. Actions should be taken by all agencies to remove relevant flags and markers.

However, any perpetrator who has previously been the subject of a MARAC referral should always be considered to be high risk.

If the referring Agency is not present, the Chair to feed back to the referring agency that it was the consensus of the agencies present at MARAC that the case was not considered to be high risk.

If the case has been referred without consent and any agency representative, including the Chair, believes the case not to be high risk, it is important that this is mentioned before any information is shared. If nobody has anything to share that would indicate that the risk is high, then the case should not be heard. Actions should be taken by all agencies to remove relevant flags and markers. This is very important as the information sharing gateways without consent apply to high risk cases only.

If the referring Agency is not present, the Chair to feed back to the referring agency that it was the consensus of the agencies present at MARAC that the case was not considered to be high risk and was not heard. However, if at least one agency believes it to be high risk, then the case should be heard.

9.5 **Action Planning**

A tailored action plan will be developed at each MARAC to increase the safety of the victim, children, perpetrator, other vulnerable parties and any staff.
If victims and their children are at high risk of being significantly harmed or murdered, agencies must agree to prioritise the actions assigned and deliver them on the day of the MARAC or as soon as possible thereafter.

Agencies will consider whether any actions can be taken in relation to managing the behaviour of the perpetrator.

The action plan details any actions volunteered at the MARAC by individual and identifies the specific risk the action is related to.

Process of forming the Action Plan:

- When all the information has been shared the Chair will summarise the risks
- The Chair will then invite each agency representative in turn to volunteer any actions they believe may contribute to reducing an identified risk.
- Agencies should ensure that their actions are SMART (Specific, Measurable, Achievable, Realistic and Timely).
- Agency representatives must identify the specific risk the action is aimed at reducing.
- Agency representatives must set their own timescales in relation to individual actions having due regard for the identified risk notwithstanding clause. However, a default timescale of 7 days is assumed as a default maximum period.
- Agencies are expected to complete actions within the timescale agreed at the MARAC.
- Agencies are responsible for their own actions and are expected to keep complete records in relation to all MARAC actions on their own case management systems.
- It is critical to any risk management process that identified actions volunteered by individual agencies are completed otherwise the process becomes a meaningless exercise. This becomes doubly important within a process that does not advocate automatic review of cases unless a repeat incident is reported.
- In the event that there are difficulties in completing an action, please refer to clause 3.4
- The Chair will request agencies to identify any incomplete actions from the Action Plan for the previous MARAC at the beginning of each MARAC.

9.6 **Administration**

GMP provides some administrative support for the MARAC.

Subject to available resource GMP will:

- Prepare an Action Plan following the meeting detailing the volunteered action; the identified risk the action relates to and the timescale volunteered for completion of the action
- Upload the Action Plan to SharePoint within one working day of the MARAC where possible.
- Make an audio recording of the meeting. That recording is stored on a secure Police system.

9.7 **Information shared at MARAC**

Information will be shared at the MARAC in accordance with the Greater Manchester MARAC Information Sharing Agreement which forms part of this MARAC Operating Protocol.

In addition a Confidentiality Statement will be read out by the Chair at the commencement of each MARAC and all agency representatives will sign a copy of the Confidentiality Statement to evidence their agreement and understanding of it and to also evidence their attendance at the MARAC.

Information shared at MARAC is strictly limited to the aims of the meeting. Agencies should only share information at the meeting that is relevant, proportionate, succinct and focussed. This falls into four main categories:

- Basic demographic information including any pseudonyms used and whether there are any children which must include their full names and their ages;
- Information on key risk indicators (see appendix section for details of risk assessment checklist) including where appropriate, professional opinion on the risks faced;
- Any relevant history of domestic violence or other associated behaviour (child abuse, sexual assault) by the perpetrator or victim;
- The 'voice' of the victim. Typically the IDVA or another support agency should represent the perspective of the victim on the risks s/he faces.

Information shared at the MARAC meeting remains in the ownership of the Agency sharing it.

Information shared at the meeting cannot be used for other purposes without reference to the person/agency that originally supplied it.

At the discretion of the Chair certain agencies not normally part of the MARAC process can be invited to share information and volunteer actions in respect of specific cases if this is felt necessary to improve the safety of the victim and any children.

9.8 MARAC documentation

All documentation for the MARAC will be uploaded to SharePoint. Documents will not be distributed by email or any other means.

9.9 Criminal Procedures and Investigations Act 1996 (CPIA)

Under the CPIA Police officers are obliged to record and retain any material relevant to an ongoing investigation and/or prosecution. Should any information be disclosed during the MARAC meeting that is deemed relevant, Police officers are duty bound to request a written copy of the information and will subsequently place it onto GMP Intelligence systems and/or in the prosecution File.

9.10 Emergency MARACs

Requests for emergency MARACs or for cases to be heard at the next available MARAC when the cut-off date has passed should be made to the Chair who will either accept the case at short notice or convene an emergency MARAC or strategy meeting with all due haste.

Victim contact after the meeting - The IDVA will notify the victim of the outcome of the MARAC unless otherwise agreed at the meeting.

9.11 Equality and Diversity

Due and proper consideration should be given at MARAC meetings to all diversity issues in every case.

Equality and diversity issues will be a specific agenda item in order for the partner agencies to discuss and explore issues within this context that may affect the parties involved in any cases featuring equality and diversity issues.

The MARAC will collect information on the ethnicity, age, sexual orientation, disability and gender of victims referred to MARAC and partner agencies are required to obtain this information and note it on the referral form.

The term ‘disability’ is used to refer to a limiting long term illness, health problem or disability which limits a person’s day to day activities. A person is stated to be disabled and will be protected under the 2010 Equality Act if they have: ’a physical or mental impairment which has a substantial and long term adverse [negative] effect on their ability to carry out normal day-to-day activities’. Further guidance on Limiting Long Term Illness and Disability is available at www.safelives.org.uk

If a victim is unwilling to co-operate or volunteer equality and diversity information, this should be noted on the referral form rather than simply leaving it blank.

All agencies will ensure that MARAC referral is available to all victims of domestic abuse who meet the MARAC threshold.

10 COMPLAINTS

Complaints may be made in writing by a MARAC subject or by a participating agency.

Initial complaints must be referred to the MARAC Chair and the procedure in the event of such a complaint being received is as follows:
A letter will be sent to the complainant informing them that investigation of their complaint will be undertaken, normally within two working weeks.

The MARAC Chair will investigate the complaint and inform MARAC partners of his/her considered response.

If necessary the MARAC Chair will take advice from the Data Registrar of their or their partners' organisations and from the Information Commissioner.

The result of the investigation will be communicated in writing to the complainant.

MARAC complaints should be reported to the MARAC Steering Group.

The MARAC Steering Group will review procedures in light of the complaint and share their findings with all MARAC agencies.

Any formal complaint by a data subject regarding any stage of the process will be notified in writing to all partners.

MARAC agencies will do everything possible 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 the statutory Ombudsman.

11 BREACHES

All agencies should be aware that any breaches of this MOP may increase the risk to a high-risk victim.

Breaches of this MOP should be reported to the MARAC Steering Group by the person identifying the breach.

Reported breaches will be dealt with by the MARAC Steering Group.

12 WITHDRAWAL

Any partner may withdraw from this Protocol upon giving written notice to the other signatories.

Data that is no longer relevant should be destroyed.

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.

13 REVIEW

This Protocol will be reviewed periodically by the relevant GMP Public Protection Governance Unit with responsibility for Domestic Abuse.

APPENDIX 1
SAFELIVES-DASH Risk Identification Checklist (RIC)

SAFELIVES-DASH Risk Identification Checklist for use by IDVAs and other non-police agencies for MARAC case identification when domestic abuse, 'honour'-based violence and/or stalking are disclosed.

IMPORTANT INFORMATION

Aim of the form:

- To help front line practitioners identify high-risk cases of domestic abuse, stalking and 'honour'-based violence.
- To decide which cases should be referred to MARAC and what other support might be required. A completed form becomes an active record that can be referred to in future for case management.
- To offer a common tool to agencies that are part of the MARAC[3] process and provide a shared understanding of risk in relation to domestic abuse, stalking and 'honour'-based violence.
- To enable agencies to make defensible decisions based on the evidence from extensive research of cases, including domestic homicides and 'near misses', which underpins most recognised models of risk assessment.

How to use the form:

Before completing the form for the first time we recommend that you read the full practice guidance and Frequently Asked Questions and Answers[4]. These can be downloaded from www.SafeLives.org.uk/marac.html

Risk is dynamic and can change very quickly. It is good practice to review the checklist after a new incident.

Recommended Referral Criteria to MARAC

1. **Professional judgement:** if a professional has serious concerns about a victim's situation, they should refer the case to MARAC. There will be occasions where the particular context of a case gives rise to serious concerns even if the victim has been unable to disclose the information that might highlight their risk more clearly. ***This could reflect extreme levels of fear, cultural barriers to disclosure, immigration issues or language barriers particularly in cases of 'honour'-based violence.*** This judgement would be based on the professional's experience and/or the victim's perception of their risk even if they do not meet criteria 2 and/or 3 below.
2. **'Visible High Risk':** the number of 'ticks' on this checklist. If you have ticked 14 or more 'yes' boxes the case would normally meet the MARAC referral criteria.
3. **Potential Escalation:** the number of police callouts to the victim as a result of domestic violence in the past 12 months. This criterion can be used to identify cases where there is not a positive identification of a majority of the risk factors on the list, but where abuse appears to be escalating and where it is appropriate to assess the situation more fully by sharing information at MARAC. It is common practice to start with 3 or more police callouts in a 12 month period but this will need to be reviewed depending on your local volume and your level of police reporting.

Please pay particular attention to a practitioner's professional judgement in all cases. The results from a checklist are not a definitive assessment of risk. They should provide you with a structure to inform your judgement and act as prompts to further questioning, analysis and risk management whether via a MARAC or in another way.

The responsibility for identifying your local referral threshold rests with your local MARAC.

What this form is not:

This form will provide valuable information about the risks that children are living with but it is not a full risk assessment for children. The presence of children increases the wider risks of domestic violence and stepchildren are particularly at risk. If risk towards children is highlighted you should consider what referral you need to make to obtain a full assessment of the children's situation.

Please explain that the purpose of asking these questions is for the safety and protection of the individual concerned.

Put a cross [x] in the box if the factor is present.

Please add comments where indicated. It is assumed that your main source of information is the victim. If this is not the case please add this to your comment.

The boxes will expand as you type text into them.

There is space at the end of the form for additional information where appropriate.

[3] For further information about MARAC please refer to the CAADA MARAC Implementation Guide www.caada.org.uk.
[4] For enquiries about training in the use of the form, please email training@caada.org.uk or call 0117 317 8750.

		YES	NO	REFUSED
CURRENT SITUATION				
1.	**Has the current incident resulted in injury?** (Please state what and whether this is the first injury) Comment:			
2.	**Are you very frightened?** Comment:			
3.	**What are you afraid of? Is it further injury or violence?** (Please give an indication of what you think the abuser might do and to whom, including children). KILL (specify self, children or other) FURTHER INJURY AND VIOLENCE (specify self, children or other) Comment:			
4.	**Do you feel isolated from family/friends i.e. does the abuser try to stop you from seeing friends/family/doctor or others?** Comment:			
5.	**Are you feeling depressed or having suicidal thoughts?** Comment:			
6.	**Have you separated or tried to separate from the abuser within the past year?** Comment:			
7.	**Is there conflict over child contact?** (Please state the nature of the conflict) Comment:			
8.	**Does the abuser constantly text, call, contact, follow, stalk or harass you?** (Please expand to identify what and whether you believe that this is done deliberately to intimidate you? Consider the context and behaviour of what is being done. This question is relevant even if the parties are living together) Comment:			
CHILDREN/DEPENDANTS				
9.	**Are you pregnant or have you recently had a baby (within the last 18 months)?**			
DOMESTIC VIOLENCE HISTORY				

		YES	NO	REFUSED
10.	**Is the abuse happening more often?** Comment:			
11.	**Is the abuse getting worse?** Comment:			
12.	**Does the abuser try to control everything you do and/or is he/she excessively jealous?** Comment:			
13.	**Has the abuser ever used weapons or objects to hurt you?** Comment:			
14.	**Has the abuser ever threatened to kill you or someone else and you believed them?** Comment:			
15.	**Has the abuser ever attempted to strangle/choke/suffocate/drown you?** Comment:			
16.	**Does the abuser do or say things of a sexual nature that make you feel bad or that physically hurt you or someone else?** (Please specify who and what) Comment:			
17.	**Is there any other person who has threatened you or of whom you are afraid?** (Consider extended family if honour based violence and please specify who) Comment:			
18.	**Do you know if the abuser has hurt anybody else?** (Children, siblings, elderly relative, stranger, other partners – consider honour based violence and please specify who) Comment:			

		YES	NO	REFUSED
19.	**Has the abuser ever mistreated an animal or the family pet?** Comment:			
ABUSER				
20.	**Are there any financial issues? For example, are you dependent on the abuser for money? Has the abuser recently lost his/her job? Are there any other financial issues?** (Please specify what) Comment:			
21.	**Has the abuser had problems in the past year with drugs (prescription or other), alcohol or mental health issues that has created problems in leading a normal life?** Drugs ☐ Alcohol ☐ Mental Health ☐ Comment:			
22.	**Has the abuser ever threatened or attempted suicide?** Comment:			
23.	**Has the abuser ever breached bail/an injunction and/or any agreement for when they can see you and/or the children?** (Please specify what) Bail Conditions ☐ Non molestation/civil order ☐ Child contact arrangements ☐ Forced Marriage Protection Order ☐ Other ☐ Comment:			
24.	Do you know if the abuser has ever been in trouble with the police or has a criminal history? (If yes, please specify) Comment:			
PLEASE CALCULATE THE NUMBER OF "YES" RESPONSES and enter in the box to the right				

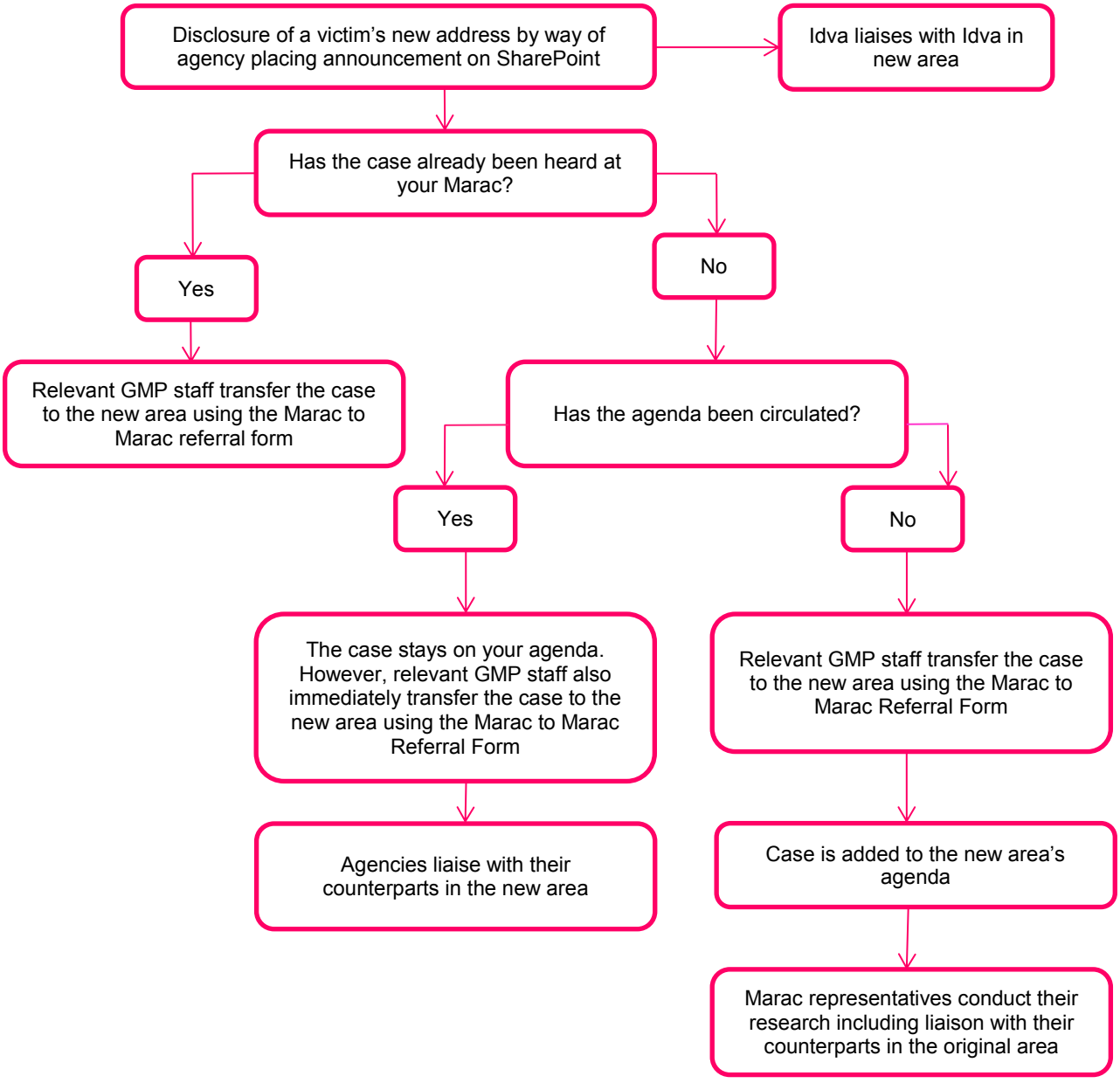
For consideration by professional:	
Is there any other relevant information (from a victim or professional), which may increase risk levels? Consider victim's situation in relation to vulnerability, disability, substance misuse, mental health issues, cultural/language barriers, 'honour'-based systems and minimisation. Are they willing to engage with your service? Describe: Consider abuser's occupation/interests – could this give them unique access to weapons? E.g. ex-military, police, pest control etc. Describe:	
Is there anything else you would like to add to this? E.g. if the victim has refused to answer any questions. Comment:	
Your name:	Date:

APPENDIX 2

Ending domestic abuse

Marac to Marac Referrals

The Referral Process



Disclosure of a new address starts the process again

Ending domestic abuse

Marac to Marac Referrals
Frequently Asked Questions

When should we make a Marac to Marac referral?
A Marac to Marac referral should be made when you become aware that a Marac victim has moved between areas, either on a temporary or permanent basis.

What information should be shared with the new Marac?
We recommend that the referring Marac send the completed Marac to Marac referral form, original Marac referral form, the Marac minutes and any other information that may be relevant to the new Marac.

Does the new Marac have to accept the referral?
Like the Marac itself, the Marac to Marac referral process does not have a statutory basis in its own right. However, we recommend that the new Marac always accepts a transferred case, regardless of the area's individual referral threshold.

Does the victim need to consent to a referral between Maracs?
No. As with a regular Marac referral, the victim's consent is not required when they are assessed to be at high risk of serious injury or homicide (the Marac to Marac referral form has space to indicate whether the victim is aware of the original referral to Marac or the transfer).

What is the role of the Idva service?
We recommend that the Idva in the original area liaises with the Idva in the new area to ensure that the victim receives support during and after a move.

What should we do if a victim is regularly being referred between the same Marac?
In some cases a victim may regularly come to the attention of agencies in two (or more) areas. In these circumstances we recommend that one area have the 'lead' responsibility for the victim; this could be the area in which the most significant risk is identified or the area in which the victim is accessing the most support.

How does this affect the local repeat referral rate?
Once a case has been referred to a Marac it is recorded within its data and flagged for 12 months. If a case has been transferred, any new incident/referral would be recorded as a repeat referral in the new area; this is regardless of where the incident occurred.

Should the Marac to Marac referral process be included in our Marac Operating Protocol (MOP) and Information Sharing Protocol (ISP)?
We recommend that the MOP specifically address the Marac to Marac transfer process. With regards to the ISP, we recommend that the process is addressed specifically or via guidance on sharing information with third parties.

Where can I get further information?
Please contact the knowledgehub@safelives.org.uk

Web www. safelives.org.uk E-mail knowledgehub@safelives.org.uk Tel 0117 403 3220

MARAC-to-MARAC referral form

MARAC referrals should only be sent using secure email or other secure method. Where available, the contact details for MARACs can be found at: safelives.org.uk/findamarac

To:	Date:

From referring area:	Contact name:
Contact number:	Contact email:

Victim information

Victim name:	Victim DOB:
Address to which victim has moved:	
Is this safe for correspondence?	
Telephone number:	
Is this safe to call?	Is there any other relevant contact information (e.g. times to call)?
Did the victim ever consent to a MARAC referral?	Is the victim aware of the case transfer?

Current IDVA service information

IDVA service:	Contact name:
Contact number:	Contact email:

Please attach additional information

Original MARAC referral form: Y / N	MARAC minutes: Y / N	Other: Y / N

Is there any additional information on the risks and needs of the victim, children or any other vulnerable party since the case was heard at the original MARAC? Is there any additional information relating to risks in the new area?

INFORMATION SHARING AGREEMENT

Version 0.5

Dated: 1st November 2016

ISA Ref No: 229

Contents

Summary Sheet

GREATER MANCHESTER MARACS INFORMATION SHARING AGREEMENT

ISA Ref: 229

Purpose:

The purpose of the information sharing is:

- To increase the safety, health and wellbeing of victims – adults and their children.
- To determine whether the perpetrator poses a significant risk to the victim, other individuals 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.
- Improve support for staff involved in high-risk domestic abuse cases.
- To ensure issues are dealt with by the most appropriate agencies / groups with relevant knowledge and practical applications.
- To assist in the statutory obligations to implement interventions for, and clarify their commitment to, the prevention or detection of Domestic Abuse and Sexual Offences; and
- To improve agency accountability.

Partners:

Detailed in Appendix [B] hereof

Date Agreement comes into force: 01/11/16
Date Agreement Review: 31/10/17

Agreement Owner: Public Protection & Serious Crime Division Superintendent Gwyn Dodd Rumney

Agreement drawn up by: Chris Woolley, Pin 63049

Protective Marking: NOT PROTECTIVELY MARKED

Location of Agreement in force:

GMP SharePoint > Document Centre > Information Sharing Repository

INFORMATION SHARING AGREEMENT

1. The Parties

THIS AGREEMENT is made the on the 1st day of November 2016.

Between the partners specified at Appendix B to this agreement.

2. Background

2.1 A MARAC is a meeting where information is shared on the highest risk domestic abuse cases between representatives of local police, probation services, health, child protection, housing practitioners, Independent Domestic Violence Advisors (IDVAs) and other specialists from the statutory and voluntary sectors. After sharing all relevant information they have about a victim, the representatives discuss options for increasing the safety of the victim and turn these into a co-ordinated action plan. The primary focus of the MARAC is to safeguard the adult victim. The MARAC will also make links with other forums to safeguard children and manage the behaviour of the perpetrator. At the heart of a MARAC is the working assumption that no single agency or individual can see the complete picture of the life of a victim, but all may have insights that are crucial to their safety. The victim does not attend the meeting but is represented by an IDVA who speaks on their behalf.

2.2 The purpose of this information sharing agreement is to facilitate information sharing between all agencies that have agreed to work together within the MARAC framework to increase the safety of victims and enable the protection of vulnerable people.

2.3 This agreement is designed to enhance existing arrangements rather than replace them, as such it should be read in conjunction with the CAADA MARAC guidance – see http://www.caada.org.uk/ and the MARAC Operating Protocol attached at Appendix A to this agreement.

2.4 MARAC is a multi-agency response to tackling domestic abuse. In a single meeting a domestic abuse MARAC combines up to date risk information with a timely assessment of a victim's needs and links those directly to the provision of appropriate services for all those involved in a domestic abuse case: victim, children and perpetrator.

3. Purpose

3.1 The purpose of the information sharing is:

- To increase the safety, health and well being of victims – adults and their children;
- To determine whether the perpetrator poses a significant risk to the victim, other individuals 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 victimisation;
- Improve support for staff involved in high-risk domestic abuse cases;

- To ensure issues are dealt with by the most appropriate agencies / groups with relevant knowledge and practical applications;

- To assist in the statutory obligations to implement interventions for, and clarify their commitment to, the prevention or detection of Domestic Abuse and Sexual Offences; and
- To improve agency accountability.

3.2 This Agreement sets out the terms and conditions under which data held by parties will be disclosed. It is entered into with the purpose of ensuring compliance with the Data Protection Act 1998. Any processing and disclosing of data must comply with the provisions of this Act.

3.3 The Purpose is consistent with the original purpose of the data collection and those registered annually with the Information Commissioner's Office.

4. Definitions

The following words and phrases used in this Agreement shall have the following meanings except where the context otherwise requires:

4.1 The expressions **"The Data Controller", "The Data Processor",** "**Personal Data**", **"Data Subject"** and "**Processing**" shall have the same meaning as identified in Section 1 of The Data Protection Act 1998, as amended by The Freedom of Information Act 2000.

4.2 "**Sensitive Personal Data**" shall have the same meaning as identified in Section 2 of The Data Protection Act 1998, as amended by The Freedom of Information Act 2000.

4.3 **"Information Commissioner**" shall have the same meaning as identified in Section 6 of The Data Protection Act 1998, as amended by The Freedom of Information Act 2000.

4.4 "**Subject Access**" shall have the same meaning as identified in Section 7 of The Data Protection Act 1998, as amended by The Freedom of Information Act 2000.

4.5 "**Aggregated Data**" means Data grouped together to the extent that no living individual can be identified from that Aggregated Data or any other Data in the possession of, or likely to come into the possession of any person obtaining the Aggregated Data.

4.6 **"A.C.P.O."** means the Association of Chief Police Officers.

4.7 **"GPMS"** means the Government Protective Marking Scheme adopted by the police service for the classification and secure handling of information; please see Appedix D for further details.

4.8 **"Agreement"** means this information sharing agreement together with its Appendices/Annexes/Schedules and all other documents attached to or referred to as forming part of this agreement.

4.9 **"The Purpose"** means the specific reasons for the processing of personal data as identified in clause 2.1 above.

4.10 The **"Information Governance Manager"** means Pat Hiorns, Information Governance Unit, Information Management Branch, Greater Manchester Police. Tel: 0161-856-2520. E-mail: pat.hiorns@gmp.pnn.police.uk

4.11 The **"Information Security Manager"** means Simon Ebbitt, Information Security Team, Information Management Branch, Greater Manchester Police. Tel: 0161-856-1324. E-mail simon.ebbitt@gmp.pnn.police.uk

4.12 **"Agreement owner"** means Public Protection Division Chief Superintendent Paul Rumney, Tel: 0161 856 2900. E-mail: paulj.rumney@gmp.pnn.police.uk.

4.13 **"Agreement drafter"** means Chris Woolley, Information Governance Unit, Information Management Branch, Greater Manchester Police. Tel: 0161 856 1156. E-mail: chris.woolley@gmp.pnn.police.uk

4.14 **"GMP"** means the Greater Manchester Police.

4.15 **"The Criminal Justice Extranet"** means a secure e-mail system rated up to the GPMS RESTRICTED marking. The following e-mail extensions are included: .pnn.police.uk, .gsi.gov.uk, gse.gov.uk, .gsx.gov.uk, .cjsm.net and .nhs.net.

4.16 **"Parties"** means the partner organisations signed up to the agreement.

4.17 **"MARAC"** means the Multi-Agency Risk Assessment Conference

4.18 **"Domestic Abuse"** means Any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality. (Family members are defined as mother, father, son, daughter, brother, sister and grandparents, whether directly related, in-laws or step-family.)

4.19 Headings are inserted for convenience only and shall not affect the construction or interpretation of this Agreement and, unless otherwise stated, references to clauses and schedules are references to the clauses of and schedules to this Agreement.

4.20 Any reference to any enactment or statutory provision shall be deemed to include a reference to the latest version of that enactment and any subordinate legislation made under it and the word 'including' shall mean including without limitation or prejudice to the generality of any description, definition, term or phrase preceding that word, and the word 'include' and its derivatives shall be construed accordingly.

5. Powers

5.1 The information described at clause 6.2 of this agreement is shared in compliance with the following legal obligations and powers:

- **The Data Protection Act 1998 s29(3)** exempts organisations from the non disclosure provisions of the Act where the information sharing is necessary and in the interests of preventing and detecting crime, and / or the apprehension and prosecution of offenders, where failure to disclose would prejudice those purposes.

- **The Crime and Disorder Act 1998**, s17 places an obligation on local authorities, police authorities and fire and rescue services to prevent and detect crime and disorder in the exercise of their functions. s115 provides a power to any person to lawfully disclose information to the police, local authority, probation services, health authority, fire and rescue service, registered social landlords or those acting on their behalf for the purposes of preventing and detecting of crime and disorder where they would not otherwise have the power to disclose information.

- **The Children Act 2004, s10** places an obligation on police, local authority, probation services, youth offending teams, health authorities, primary care trusts, and relevant partners of the children's services authority to co-operate to improve the physical, mental health, emotional well-being of children; and protection from harm and neglect.

- **The Human Rights Act 1998, Article 8** - Right to respect for private and family life, states that everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is 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, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- With the explicit consent of the victim. Where seeking consent from the victim is unlikely to prejudice the purposes of the MARAC, explicit consent should be sought. This means that the victim is fully aware and understands what they are agreeing to. Explicit consent provides both schedule 2 and 3 legitimising criteria to share sensitive personal information under the Data Protection Act 1998.

- The common law duty of disclosure, personal information may be shared where it necessary and proportionate in the interests of pursuing a crime and disorder reduction purpose, such as the protection of a MARAC subject.

- To ensure that the above legal powers, obligations and exemptions from legislation apply to share information and provide the lawful basis for disclosure the information to be shared by the partners must be necessary, proportionate and relevant for the purposes outlined at clause 3.1 and what the MARAC seeks to achieve. For example, as above information may be shared in accordance with the Human Rights Act only where it is necessary in the interests of public safety, the prevention of disorder and crime and for the protection of health, as are aims of the MARAC.

6. Information to be shared

6.1 The partners are likely to share the following information in pursuit of the purpose.

- Details of the incident, which has led to the referral.
- Details of the victim of domestic abuse.
- Details of the perpetrator of domestic abuse.
- Details of any children.
- Details of other relevant incidents involving the victim and/or alleged perpetrator.
- Details of a parent who may need help or be unable to care for a child adequately or safely.
- Details of those who may pose a risk of harm to a child or vulnerable person.
- Details of a child's health and development or exposure to possible harm.
- Any other relevant information, which is necessary to take appropriate action to protect the victim, child or vulnerable individual.
- The views of the victim. Typically the IDVA or another support agency should represent the perspective of the victim on the risks she or he faces and how best to address them.

6.2 It is recognised that the Purpose requires access to data previously protectively marked under the Government Protective Marking Scheme.

6.3 The data will be provided for the following period 01/11/16 to 31/10/17 at which time the agreement will be formally reviewed.

6.4 Ownership of the data shall at all times remain with the originating Data Controller.

7. Uses, Disclosure and Publication

7.1 The specific procedures relevant to this Agreement are contained in Appendix A – The MARAC Operating Protocol.

7.2 In particular, the information shall be used to formulate an action plan to increase the safety of the victim and their family, this includes but is not limited to: Co-ordinating a response that ensures appropriate resources are offered by MARAC partner agencies.

- Jointly constructing and implementing a risk management plan that provides professional support to all those at risk and that reduces the risk of harm.
- Determining whether the perpetrator poses a significant risk to any particular individual or to the general community.
- Ensuring compliance with statutory obligations, guidance and performance indicators;
- Identifying high-risk victims of Domestic Abuse and to attempt to prevent further escalation of violence and abuse to threat victims/children.

- The management of threats / risk of crime, disorder and alcohol / substance misuse in victims of Domestic Abuse.

- The evaluation of outcomes of interventions towards the protection of serious harm or homicide to a victim and to increase the safety, health, and wellbeing of adult victims and their children.

7.3 The data will be used solely for the Purpose and the Parties will ensure that all the data is accessed only as identified within this Agreement, the provisions of which must be complied with.

7.4 The data will NOT be disclosed to any third party unless strictly in accordance with the Purpose.

7.5 The data will NOT be matched with any other data obtained from any other source, unless strictly in accordance with the Purpose.

7.6 Clause 7.4 above shall not apply where disclosure of the data is ordered by a Court of competent jurisdiction, or subject to any exemption under the Act, where disclosure is required by a law enforcement agency or regulatory body or authority, or is required for the purposes of legal proceedings. Where information is required to be disclosed in these circumstances and the Personal Data to be disclosed is identified as belonging to or originating from, another Party, that other Party shall immediately be notified in writing of the requirement for disclosure in order to allow the other Party to make representations to the person or body making the requirement.

7.7 The restrictions contained in clauses 7.4 and 7.5 shall cease to apply to any data which may come into the public domain otherwise than through unauthorised disclosure by the Parties to the Agreement.

7.8 Access to the data will be restricted to those employees of the Parties directly involved in the processing of the data in pursuance with the Purpose.

7.9 Personal Data will not be published in an identifiable form unless the data subjects concerned have given their consent and in conformity with other safeguards laid down by domestic law.

8. Roles and responsibilities under this agreement

8.1 Detailed roles and responsibilities are set out at Appendix A – MARAC Operating Protocol.

8.2 Each partner must appoint a single point of contact (SPoC) who will work together to jointly solve any problems arising from the information sharing and to actively improve the effectiveness of the information sharing initiative.

8.3 Greater Manchester Police will maintain a list of partners to this agreement and SPOCs for each of the partners.

9. Data Protection and Subject Rights

9.1 The use and disclosure of any Personal Data shall be in accordance with the obligations imposed upon the Parties to this Agreement by the Data Protection Act 1998 and the Human

Rights Act 1998. All relevant codes of practice or data protection operating rules adopted by the Parties, including the Framework code of practice for sharing personal information published by the Information Commissioner, will also reflect their data protection practices.

9.2 The information sharing has been assessed for compliance with data protection and human rights legislation for further details of these assessments please contact the agreement owner and agreement drafter.

9.3 The Parties agree and declare that the information accessed pursuant to this Agreement will be used and processed with regard to the rights and freedoms enshrined within the European Convention on Human Rights. Further, the Parties agree and declare that the provision of information is proportional, having regard to the purposes of the Agreement and the steps taken in respect of maintaining a high degree of security and confidentiality.

9.4 The Parties undertake to comply with the provisions of the Data Protection Act 1998 and to notify as required any particulars as may be required to the Information Commissioner.

9.5 If any Party receives a request under the Subject Access provisions of the Data Protection Act 1998 and Personal Data is identified as belonging to or originating from, another Party, the receiving Party will contact the other Party to determine if the latter wishes to claim an exemption under the provisions of the Act.

9.6 It is acknowledged that where a Data Controller cannot comply with a request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request, unless;

a) The other individual has consented to the disclosure of the information to the person making the request; or

b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to:

- Any duty of confidentiality owed to the other individual;
- Any steps taken by the Data Controller with a view to seeking consent of the other individual;
- Whether the other individual is capable of giving consent;
- Any express refusal of consent by the other individual.

9.7 Where any Party receives a Notice under Section 10 of the Data Protection Act 1998, and the Personal Data to which the Notice applies is identified as belonging to or originating from another Party, the receiving Party will contact that other Party to ascertain whether or not they wish to make any representations about a response to, or compliance with, that Notice. All Parties recognise that a response to such a notice must be provided within 21 days and agree to make any representations as soon as possible to enable this deadline to be met.

9.8 The Parties agree to give reasonable assistance as is necessary to each other in order to enable them, in accordance with statutory obligations, to:

- Comply with requests for Subject Access from Data Subjects;
- Respond to Information Notices served upon them by the Information Commissioner;
- Respond to complaints from Data Subjects;
- Investigate any breach or alleged breach of the Act;

in accordance with statutory obligations under the Data Protection Act 1998.

9.9 The Parties agree to allow other Parties to conduct periodic checks to confirm compliance with this Agreement provided that reasonable notice of the intention to conduct such a check is given.

10. Freedom of Information (FOI)

10.1 This agreement shall be subject to disclosure under the provisions of FOI and GMP shall be obliged to disclose it, and associated documents to anyone requesting them under Freedom of Information.

10.2 Additionally, if any Party receives an application for access to any information under the provisions of the Freedom of Information Act 2000 and that information is identified as having originated from another Party, that Party will be contacted to determine whether it wishes to claim an exemption under the provisions of the legislation or to issue a response neither to confirm nor deny that information is held.

11. Security

11.1 The Parties recognise that the Chief Constable has obligations relating to the security of data in his control under the Data Protection Act 1998, the Code of Practice for Information Security Management (ISO/IEC 27001:2005), the ACPO Information Community Security Policy, the Manual of Protective Security and the GPMS. These obligations are audited by the Police Information Assurance Board.

11.2 The Parties agree to apply appropriate security measures, commensurate with the requirements of The Seventh Data Protection Principle, which states that: “appropriate technical and organisation measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”. In particular, they shall ensure that measures are in place to do everything reasonable to:

- Make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport
- Deter deliberate compromise or opportunist attack, and
- Promote discretion in order to avoid unauthorised access

11.3 The Parties are required to handle all data received in accordance with the protective marking shown, if no marking is shown the data should be handled in accordance with at least RESTRICTED GPMS marking, please see Appendix D for further details of all information security handling requirements. For example, all manual papers should be stored within a lockable cabinet within a secure building, with access only granted to those individuals pursuant to the Purpose.

11.4 Where data is shared by e-mail the Parties agree to set up a secure e-mail account within the Criminal Justice Extranet, if they do not operate within the Extranet already, using the guidance attached at Appendix E so that data can be shared securely between the Parties in a convenient and auditable manner.

11.5 Parties sharing information reserve the right to conduct a site security assessment to establish that an appropriate level of security is provided by those parties receiving information at a time and date convenient to both Parties prior to the commencement of the sharing. If reasonable recommendations are made these should be implemented. Failure to

provide sufficient guarantees in respect of adequate security measures may result in the termination of this Agreement.

11.6 The Parties agree to comply with all reasonable requirements concerning the storage, access or use of any Data as may from time to time be made by any party who shares information.

11.7 The parties undertake not to use the services of any sub-contractors in connection with the processing of the Data without the prior written approval of the Chair of the MARAC, furthermore any access to the premises used to process the Data by maintenance or repair contractors, cleaners or other non-authorised persons must be closely supervised to ensure that there is no access to the Data.

11.8 Any information security breaches, including threats, weaknesses, incidents of unlawful processing, accidental loss, destruction or damage to data should be reported to the originating partner using the contact information identified at 9.8 as per Appendix F Information Security Breach Guidance using the Information Security Breach Report attached at Appendix G.

11.9 The partners recognise that additional powers to serve assessment notices on public authorities have been granted to the Information Commissioner, which allow access to premises, records and staff etc to inspect security and compliance with the Data Protection Principles. New powers also allow the Information Commissioner to levy fines up to £500,000 for any breaches.

11.10 The partners recognise the importance of ensuring that the Information Commissioner and individual Data Subjects can benefit from early notification of data security breaches, however, they are mindful that disclosure can sometimes be detrimental to the subject and / or the public interest depending upon the sensitivity of the information involved. The partners agree to adopt the procedure set out in Appendix F Information Security Breach Guidance when considering notification of security breaches to the Information Commissioner and / or individual Data Subjects

12. Review, Retention and Disposal of Data

12.1 The Parties agree that all data supplied pursuant to this agreement will be retained for no longer than is necessary in all the circumstances of each case.

12.2 When the data supplied under this agreement is no longer required, it will be securely disposed of.

13. Confidentiality

13.1 The Parties agree to treat the data received by them under the terms of this Agreement as confidential and shall safeguard it accordingly. Respect for the privacy of individuals will be afforded at all stages of carrying out the Purpose.

13.2 The parties shall ensure that any individuals involved in the Purpose and to whom police data is disclosed under this Agreement are aware of their responsibilities in connection with the use of that data.

13.3 For the avoidance of doubt, the obligations or the confidentiality imposed on the Parties by this Agreement shall continue in full force and effect after the expiry or termination of this Agreement.

13.4 Further to the above, the MARAC confidentiality statement refered to in the MARAC Operating Protocol at Appendix A shall be read out at the start of the MARAC.

14. Review of the information sharing agreement

14.1 This Agreement is based on the guidance provided by ACPO and the Home Office on the Management of Police Information and on the Manual of Guidance for Data Protection published by the ACPO Data Protection Portfolio Group. The Agreement Owner with the assistance of the GMP Information Governance Unit, in conjunction with partner agencies, will initiate a review of the agreement six months after initiation and annually thereafter.

14.2 The guidance and forms attached at Appendix C – The Review Process shall be followed and utilised when the agreement is due for review.

15. Notification of New Signatories and Amendments to the Agreement

15.1 Information will not be disclosed to third parties except as specified in this Agreement. Notification of new partners signing the agreement will be made by email to the SPOC for each agency.

15.2 Amendments to this Agreement must also be subject to the ISA Change Control Procedure.

16. Complaints and Breaches

16.1 If any party receives a complaint regarding the use or disclosure of information exchanged under this Agreement then:

- If it concerns information obtained from GMP, the complaint will be referred to the Information Governance Manager.
- If it concerns information from any of the other Parties it will be referred to an appropriate information governance contact from that partner.

16.2 It is recognised that complaints may have serious implications for other Parties and the referrals described in Clause 16.1 above, will be made as soon as possible and in any case within 7 days.

17. Disputes

17.1 In the event of any dispute or difference arising between the Parties to this Agreement, they shall appoint representatives to meet within 20 days of receipt of a written request from either Party to the dispute in an effort to resolve the dispute or difference in good faith.

17.2 The Parties will, with the help of the Centre for Dispute Resolution (http://www.cedr.co.uk), seek to resolve disputes between them by alternative dispute resolution. If the Parties fail to agree within 56 days of the initiation of the alternative dispute resolution procedure, then the Parties shall be at liberty to commence litigation.

17.3 The validity, construction and interpretation of this Agreement and any determination of the performance which it requires shall be governed by the Laws of England and the Parties hereby submit to the exclusive jurisdiction of the English Courts and English law.

18. Term, Termination and Variation

18.1 Any party disclosing information may at any time, by notice in writing, withdraw from this agreement forthwith if a party receiving their information is found to be in material breach of any obligation under this agreement.

18.2 Any Party may leave this Agreement by giving 30 days notice in writing to the other Parties.

18.3 Any proposed changes to the Parties involved in this Agreement, to the purposes of the information sharing, the nature or type of information shared or manner in which the information is to be processed and any other suggested changes to the terms of this Agreement must be notified immediately to the Agreement Owner before any change is put into effect, so that the impact of the proposed changes can be assessed.

18.4 No variation of the Agreement shall be effective unless it is contained in a written instrument signed by all Parties and annexed to this Agreement.

18.5 A review of this information sharing agreement shall take place after six months of commencement and then annually thereafter. All parties to this agreement agree to take part and fully cooperate in this review.

19. Indemnity

19.1 In consideration of these arrangements for sharing information for the Purpose any party receiving information undertakes to indemnify and keep indemnified any party that has disclosed information to them against any liability, which may be incurred by the disclosing party, as a result of the receiving party breaching the terms of this agreement.

19.2 Provided that this indemnity shall not apply:

a) Where the liability arises from information supplied by the disclosing party that is shown to have been incomplete or incorrect, unless the disclosing party establishes that the error did not result from any wilful wrongdoing or negligence on his part

b) Unless the disclosing party notifies the receiving party as soon as possible of any action, claim or demand to which this indemnity applies, commits the receiving party to deal with the action, claim or demand by settlement or otherwise and renders the receiving party all reasonable assistance in so dealing;

c) To the extent that the disclosing party makes any admission, which may be prejudicial to the defence of the action, claim or demand.

19. Signatures

19.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement and to comply with relevant legislation.

Name of Partner:

Signed by:

Signature:

Date:

19. Signatures

19.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement and to comply with relevant legislation.

Name of Partner:

Signed by:

Signature:

Date:

19. Signatures

19.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement and to comply with relevant legislation.

Name of Partner:

Signed by:

Signature:

Date:

19. Signatures

19.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement and to comply with relevant legislation.

Name of Partner:

Signed by:

Signature:

Date:

19. Signatures

19.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement and to comply with relevant legislation.

Name of Partner:

Signed by:

Signature:

Date:

Appendix B – List of signatories

Appendix C - The Review Process

Stages to be covered in the review process:

1. Are all contact details correct?

Each signatory organisation has a responsibility to maintain up-to-date contact details of the key individuals operating or managing the sharing activity. When a change in personnel occurs, the partners in question should ensure that the other parties are aware of the change and update the agreement accordingly.

2. Is the information sharing agreement still useful and fit for purpose?

This is an opportunity to ensure that the correct information is being shared and that the ISA does not need to be adjusted to reflect any change in needs. Where a change is required this must be agreed by the partner agencies and an addendum made to the ISA, indicating the reasons for the change(s). This will form part of the audit trail. If substantial changes are required then a new ISA may be necessary.

3. Has the review identified any emerging issues?

The review provides an opportunity to discuss any problems that may have arisen. Reviewers will also need to be aware of any changes in the legislation that may impact upon the sharing and the agreement. Reviews can also be used to identify any gaps in the information-sharing regime and identify requirements for other agreements.

4. Are the procedures for ensuring the quality of information being adhered to and are they working in practice?

The review should identify if any of the information-sharing partners are failing to meet agreed standards in areas such as data accuracy, data retention, timely provision of information and data security etc.

5. Is the data still shared in the manner specified in the agreement?

Has there been any changes to the way in which the information is shared, if so the agreement should be amended to reflect these changes to ensure that all partners are clear regarding the information sharing procedures.

6. Are the provisions for guaranteeing individuals' DP rights adequate?

The review should highlight the accuracy and continuing relevance of the fair processing notices (privacy policies) and the effectiveness of procedures for dealing with subject access requests

7. Extending / terminating the agreement

At the end of the review, a decision should be made on whether to extend the ISA for a further period (typically 1 year) or whether to terminate it. Any decision should be recorded with the reasons for choosing a particular course of action clearly stated.

The form below should be circulated to each of the partners for their comments prior to the commencement of the ISA review.

Review and Renewal Form

NAME OF AREA MULTI AGENCY RISK ASSESSMENT CONFERENCE					
[Name of partner] comments					
1. Are all contact details correct?					
2. Is the information sharing agreement still useful and fit for purpose?					
3. Has the review identified any emerging issues?					
4. Are procedures for ensuring that quality of information being adhered to and are they working practice?					
5. Is the data still shared in the manner specified in the agreement?					
6. Are the provisions for guaranteeing individuals' DP rights adequate?					
7. Extending / terminating the agreement					
Date		Name		Signature	

Appendix D - Guide to the handling of protectively marked material

You are required to handle the disclosed material in accordance with the requirements below. The appropriate protective marking should be shown in capitals at the top and bottom of the information, if it is not all information should be handled in accordance with at least RESTRICTED marking.

- The material should be accessed on a need to know basis only. Only approved personnel should have access to the data.
- Security measures must be in place to prevent unauthorised access and unlawful processing of information.
- Implement a clear desk and screen policy whilst the disclosed material is in your possession. Use of a password protected screensaver after 3 minutes of inactivity is highly recommended.
- Where data is held on portable media or laptops encryption tools should be employed and the media should remain under the positive control of approved personnel. Positive control means on their person and in their sight.

Storage of material	
RESTRICTED	Should be stored behind at least one enforceable barrier in a secure building. For example, stored in a locked cabinet in a secure building.
CONFIDENTIAL	Should be stored behind at least two enforceable barriers. For example, stored in a locked cabinet, within a locked office in a secure building.
Movement of material	
RESTRICTED	**Post** - The material may be sent by post or courier in a sealed envelope, which does not show any protective marking. **E-mail** - The material may only be sent using the CJX network. (i.e. those e-mail addresses containing .pnn, .gsi, .nhs net and .cjsm) See Appendix L. **Fax** – May be used in cases of operational urgency if due caution is exercised. I.e. send cover sheet first and await response before sending.
CONFIDENTIAL	**Post** - The material may be sent by post or courier providing it is placed in two sealed and addressed envelopes. The protective marking should be shown on the inner envelope only, the outer envelope should include a return address. **E-mail** - Not to be used without approved encryption service. **Fax** – Not to be used unless approved encrypted fax service available.
Disposal of material	
RESTRICTED	**Disposal of waste paper -** Destroy using a cross cut shredder or so that it cannot be reconstituted. Keep waste secure before shredding and whilst unattended*. **Disposal of magnetic media -** Floppy disk - dismantle then cut the disk into quarters and dispose of with normal waste*. **Optical Media** - destroy completely - disintegrate, pulverise, melt or shred*. **Reuse of Media (Hard Drives etc)-** Triple overwrite using CESG approved software.
CONFIDENTIAL	**Disposal of waste paper -** Destroy using a cross cut shredder or so that it cannot be reconstituted. Keep waste secure before shredding and whilst unattended*. **Disposal of magnetic media -** Floppy disk - dismantle then cut the disk into quarters and dispose of with normal waste*. **Optical Media** - destroy completely - disintegrate, pulverise, melt or shred*. **Reuse of Media (Hard Drives etc) -** Triple overwrite using CESG approved software. *Alternatively please send the material to the Information Governance Unit, Chester House, Old Trafford, M16 0RE, in accordance with the details above so that it can be securely disposed of.

For further details on any of these information security requirements please contact the Force Information Security Manager on 0161 856 1324.

Appendix E - Guide to setting up a secure e-mail account

There is an obligation on GMP, the CPS and other partners who have adopted the GPMS to share information, which may attract a protective marking of Restricted and above with partner agencies. Many partner agencies use secure e-mail services such as .pnn, .gsi and .cjsm nhs.net.

What about those partner agencies who do not have access to these secure e-mail facilities. The Criminal Justice Extranet (CJX) Community offer a possible solution via their Criminal Justice Secure E-mail (CJSM) facility. This CJSM facility is available for most government agencies and partners.

This e-mail facility was originally set up for the Crown Prosecution Service and allows individuals secure access to a mailbox which sits within the secure government network (.pnn and .gsi)

The web address where users can register for this secure and free of charge account is: http://www.cjsm.cjit.gov.uk

Once users have registered their details for this service and it has been accepted then they are given a secure e-mail address and can access their mailbox through a login website: http://www.cjsm.net the usage of the website is similar to a number of free e-mail services such as yahoo.

For any enquiries phone the CJSM Helpline on: 0870 010 8535

Any information which is sent from our network to CJSM account will only travel within the secure government network, which means that the chance of the e-mail being intercepted on route is negligible. This form of e-mail is approved by CESG.

It is for the individual department to ensure that they have sharing protocols in place with the partner agencies recipients to ensure that they have adequate controls in place to protect the information that has shared with them.

Appendix F - Information security breach guidance

Data controllers must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data. The specific security measures to be implemented by the partners to this agreement are set out at Section 10 – Security. However, if an information security breach does occur the following guidance should be followed.

The specific circumstances in which a breach will take place and the severity of the incident will vary, as such the appropriate action to take following the incident will depend on those circumstances. This guidance note should however assist in deciding the appropriate course of action should an information security breach occur.

An information security breach can occur for a number of reasons, such as:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances, such as fire or flood
- Hacking attack
- “Blagging” offences, where information is obtained by social engineering or other deceitful methods

Requirements

1. The SPOC should ensure a record is maintained of all information shared with partner agencies for audit purposes. This will assist in knowing what data has been lost or compromised.

2. Avoid the use of portable media to share / store data in information sharing initiatives, this will go missing the question is when. Information should be shared in accordance with the terms and conditions of this agreement.

3. When transferring data to a partner SPOC advise that data is being sent and ask for confirmation on receipt.

4. Submit an Information Security Breach Report to the data owner and any other relevant partner if an information security incident occurs. If the incident involves information which is believed to have originated from GMP the Information Governance Manager and the Information Security Manager should be fully updated using the template seen at Appendix N.

Containment and recovery

The relevant SPoCs and individuals identified at clause 8.9 or a representative on their behalf should meet without delay. If the incident involves information for which GMP is identified as the data owner the Information Security Manager should be included. This group shall be known as the “Security Breach Response Planning Group”, their priorities are as follows:

1. The first priority of the Group is to ensure that the breach has been contained and that no further data can be lost or compromised in the same manner. This could involve: attempts to locate the lost equipment / information, changing access codes, passwords, storing the data in a new location or terminating the information sharing initiative due to breaches of the information sharing agreement.

2. Decide who will take the lead in investigating the incident and ensure that they have the appropriate resources.

3. Decide who else needs to be made aware of the incident and clearly inform them what they are expected to do to assist in the containment exercise.

4. Consider what can be done to recover losses, as well as physical recovery of lost equipment, this could involve use of the relevant SPOC's audit folder, (where all data shared is recorded) and / or use of backups to restore lost or damaged data.

5. Where appropriate, report the incident to the police as a crime to be investigated as a criminal matter.

Assessment of risk

Some information security breaches will simply result in inconvenience to those who need the data to conduct their job effectively, whilst compromise of some police data may lead to a direct risk to safety of the data subjects. The following shall then be considered:

1. What GPMS marking is the information lost?

2. Is the information personal data / sensitive personal data?

3. Is the data encrypted / password protected? Is the key / password also likely to be compromised? i.e. was the encryption key stored with the data / equipment?

4. What has actually happened to the data, has it simply been damaged or has it been deliberately stolen? This poses a different type and level of risk.

5. What is the volume of the information lost? It is not necessarily the case that the greater the volume the greater the risk, but it is certainly a determining factor in the overall risk assessment.

6. What harm may come to the data subjects? Will compromise of the information lead to safety risks? i.e. has data relating to witnesses / victims of crime been compromised?

7. Will policing purposes, e.g. an investigation be compromised as a result of the incident?

8. Are there wider consequences to consider, for example loss of public confidence in an important service?

Notification of breach

Informing individuals and organisations that an information security breach has occurred can be an important part of the response to an incident. Notification should have a clear purpose and is not an end in itself. For example, to enable individuals to take steps to protect themselves or allow the Information Commissioner to provide advice and guidance, deal with complaints and perform regulatory duties. At present there is no obligation which expressly requires data controllers to notify a breach, but the following guidance may lead towards notification:

1. Will notification assist in ensuring compliance with the Seventh Data Protection Principle?

2. Would notification to the individual assist them? For example, could acts be taken by the individual to help mitigate the potential risks associated with the loss or compromise?

3. If the breach involves personal data and the Information Commissioner is notified they can then be used as a useful resource for advice and guidance, and may as a result of being notified take less severe regulatory action.

4. The potential harm to individuals should be the overriding consideration in deciding whether to notify the Information Commissioner or the data subjects themselves. The extent of harm is determined by both volume and sensitivity of the information lost or compromised. Where there is

little risk to individuals and the volume is considered to be small there is no need to report the breach. However, the advice from the Commissioner is that where the data controller is unsure there should be a presumption to report. A balance test needs to be conducted regarding the potential impact, for example would notification act as “tipping off” or potentially prejudice the safety of an individual.

5. The Information Commissioner does not see it as their responsibility to publicise details of an information security breach not already in the public domain, therefore incidents may be reported without fear of the details being made public. However, where regulatory action, i.e. enforcement action is taken this is usually made public.

6. Dangers of over notifying, not every incident will require notification as this may lead to disproportionate effort and / or unnecessary stress to the individuals involved.

If the decision has been taken to notify the Group need to consider who is going to be notified, the timing of the notification, what they are going to be told and how the message is going to be communicated. It is important to bear in mind the security of the message as well as the urgency of the situation.

If individuals are to be notified the SPoCs shall be responsible for compiling a list of the names of all individuals affected or reasonably believed to be affected, their address or other appropriate contact details. It is recommended that the following be included in a notification message:

1. A description of how and when the breach occurred.

2. A description of what data has been lost or compromised.

3. Details of what actions have already been taken to contain the data loss or compromise.

4. Specific and clear advice regarding what they can do to protect themselves, mitigate the potential risks to them and what the Group is willing to do to help protect them.

5. Provide a way in which the Group or another individual can be contacted for further information about what has happened, advice and guidance.

Where the safety of the data subjects may be at risk they shall notified in the most expedient time possible and without unreasonable delay. Notification may be delayed where there are no concerns regarding risk to safety and if as a result of notification a criminal investigation or other policing purpose could be compromised.

If the Information Commissioner is to be notified it is recommended that the following should be included:

1. The type of information and the number of records.

2. The circumstances of the loss or compromise.

3. Actions taken so far or planned to mitigate the effect to the individuals involved, including whether they have been notified.

4. Details of how the breach is being investigated.

5. Details of the security measures in place when the information security breach occurred.

6. Details of remedial action to contain the loss or compromise of information.

7. Details of who else has been notified of the incident.

Evaluation

It is important not only to investigate the causes of the information security breach but also to evaluate the effectiveness of the Group's response, to ascertain what problems occurred and how this process can be improved should another information security breach occur. Similarly following the above guidance and then continuing as usual is not acceptable if problems in the information sharing, inadequacies in the information sharing agreement, training and handling by partner agencies have been identified.

Appendix G - Information security breach report

From

To

The Information Security Manager
Information Security Team
Information Management Branch
Greater Manchester Police Headquarters
Boyer Street
Old Trafford
Manchester
M16 0RE

Cc The Information Governance Manager

Date

Location of Premises:

Person Reporting:

Date and time of occurrence/came to notice:

Brief details including impact :