



## **Multi Agency Risk Assessment Conference (MARAC) Partnership Information Sharing Guidance**

### **1. Introduction**

The Multi-Agency Risk Assessment Conferences (MARACs) focus on high risk victims of domestic violence. The National Indicator (NI 32) definition describes how activity by police and local partners should be focused on protecting the most vulnerable victims from serious harm. Domestic violence victims currently have the highest level of repeat victimisation, often with the severity of incidents escalating over time. Victims of domestic violence referred to a MARAC will be those who have been identified (often by the police) as high or very high risk (i.e. of serious injury or of being killed) based on a common risk assessment tool that is informed by both victim and assessor information. It is recommended that MARACs are held at fortnightly intervals, where each high risk case referred is discussed by partners attending and information relevant to the immediate safety of the victim is shared. MARACs are currently held every six weeks in Eastbourne and in Hastings.

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

**1.1** This document aims to facilitate information sharing between all agencies who have agreed to work together within the MARAC framework in East Sussex to increase the safety of victims, enable the protection of vulnerable people and reduce crime and disorder locally.

**1.2** This guidance document should be read in conjunction with the East Sussex MARAC Operating Protocol (v8) that sets out how partner agencies contribute to the effective operation of the MARAC, setting out the aims, membership and process of the MARAC, stating the accountability, governance and performance management structures of the framework.

**1.3** The guidance should also be read in conjunction with the Sussex MAPPA (multi-agency public protection arrangements) & MARAC Protocol (V1.5)<sup>1</sup>.

**1.4** The Sussex-wide Information Sharing Agreement<sup>2</sup> (currently being rewritten as the South Coast Information Sharing Protocol) and the Criminal Justice System Information Sharing Guidance (2009<sup>3</sup> Appendix A) outline the overarching data sharing principles and clarify the understanding between organisations on each party's responsibilities towards each other and data subjects. The CJS Guidance also details agencies obligations in relation to The Data Protection Act 1998 and the Human Rights Act, 1998 and provides guidance as to whether it is appropriate to share information.

**1.5** Also relevant is the East Sussex Domestic Violence Information Sharing Guidance v2 Jan 10.

**1.6** This document in no ways constitutes legal advice. Specific legal advice should be sought in cases where there is any doubt as to whether information sharing is appropriate.

**1.7** This Information Sharing Guidance should be reviewed at least annually by the MARAC Steering Group in conjunction with the annual review of the MOP.

**1.8** Key Partners to the MARAC are:

- a. Action for Change
- b. Community Health Services (NHS East Sussex)
- c. CRI Domestic Abuse Service
- d. East Sussex County Council Children's Services
- e. East Sussex Safer Communities Team
- f. Eastbourne Borough Council – Housing Department
- g. Eastbourne Downs and Weald Community Substance Misuse Team
- h. Hastings and Rother Community Substance Misuse Team
- i. Hastings Borough Council – Housing Department
- j. Lewes District Council – Housing Department
- k. Refuge (Eastbourne, Hastings, Lewes and Wealden)
- l. Rother District Council
- m. St Jude's Refuge (Rother)
- n. Surrey & Sussex Probation Trust
- o. Sussex Partnership NHS Foundation Trust
- p. Sussex Police
- q. Wealden District Council – Housing Department

**1.9** Other agencies (e.g. Adult Social Care, Youth Offending Team [YOT] and Local Safeguarding Children Board [LSCB]) will be invited on a case-by case basis as appropriate and where a referral has been made by that agency or because additional professional support is required.

**1.10** Agencies agreeing to the principles of the guidance and to signing the protocol are agreeing to share information in all domestic violence situations relating to MARAC, to comply with all relevant legislation, to seek their own legal advice and to use the data disclosed only for the agreed purpose.

**1.11** Agencies are agreeing to share information in high risk situations, to comply with all relevant legislation, to register with the information Commissioners Office to seek their own legal advice and to use the data disclosed only for the agreed purposes.

**1.12** Each agency across East Sussex will nominate designated information sharing officers who can provide advice and assistance to their own agency in response to data sharing requests made. The Officer must be of sufficient standing within the signatory agency to have a coordinating and authorising role as they are responsible for ensuring that the agency they represent obeys the guidance and all relevant legislation.

**1.13** The multi-agency co-ordinated response to domestic violence across East Sussex enables the use of an integrated case management system, Modus. The aim is to ensure that all agencies involved in work in an integrated and co-ordinated way to achieve and improve the safety of adults and children experiencing domestic abuse and to enable agencies to work in partnership and share appropriate information in order to achieve that.

**1.14** Responsible information sharing enables:

- Timely action to be taken to protect victims and safeguard children from further abuse;

- Comprehensive identification of risk and safety planning based on a full account of the circumstances of each client;
- An effective combination of advice, support and advocacy at the right time based on the clients history and need;
- The avoidance of the client having to repeat details of their history or experience of domestic violence each time they encounter a different agency or worker.

## **2. Reasons to Share Data**

Working together in partnership within the domestic violence framework in East Sussex to increase the safety of victims, enable the protection of vulnerable people and reduce crime and disorder locally. The sharing of information is vital to safeguarding and promoting the welfare of victims of domestic violence and also their children.

It is often only when information from a number of sources has been shared and is put together that it becomes clear that a child or a vulnerable adult is at risk of or is suffering harm.

## **3. Legal Grounds for Sharing Information**

In addition to legislation referred to in the CJS document, CAADA<sup>4</sup> provide guidance in relation to:

### ***a) Safety***

Factors of risk relating to the adults and any children, even low risk must be considered.

### ***b) Consent***

Where consent is in place, information can be disclosed. Where there is no consent, a professional judgement must be made, balancing whether

- There is legal authority to disclose;
- Duty of confidentiality;
- Risks to those affected;
- Pressing need;
- Need of other agencies to know;
- Proportionate response.

### ***c) Making a decision***

Disclosing, recording the decision and considering ways to reduce risk to the survivor and/or children and ways to help the client access help directly. Any concerns relating to information sharing and the appropriateness of sharing specific information should be referred to the Designated Information Sharing Officers within the specific agency.

## **4. Types of Information Shared**

Information will be shared in various formats, and stored electronically in Modus, the electronic case management system used by the partnership. All information relating to victims, children, and where appropriate the perpetrator of domestic violence will be entered into the system. The incident case work and case outcome will be updated in the system throughout the lifetime of the case.

The types of information to be shared (defined in the CJS document) are:

- Non-personal data

- De-personalised data
- Personalised data
- Sensitive personalised data

**4.1** Data will be used to construct a unique safety plan that will attempt to address the risks faced by the adult victim and children. It may also cover risks faced by agency staff, neighbours or colleagues and indeed the perpetrator.

## **5. Data Routinely Shared In MARAC**

Each MARAC attendee will contribute to the case discussions where appropriate and will inform the meeting as to the information their own agency can provide to assist discussions.

**5.1** It is best practice to inform individuals that there is intention to share information in relation to their case so that sharing takes place with their knowledge. In some circumstances however, it might be appropriate not to inform for example where this will:

- Place a child at increased risk of significant harm
- Place an adult at risk of serious harm or
- Prejudice the prevention or detection of a serious crime
- Lead to unjustified delay in making enquiries about allegations of significant harm

**5.2** It might be the case that the relevance of a particular piece of information does not become apparent until other matters are disclosed during the MARAC meeting, for example:

- A woman may have had one or more terminations of pregnancy. This may not seem relevant, but it may be disclosed during the meeting if it is believed that she had been raped. If the timing correlates, the decision to disclose the terminations may be made
- A victim may have made one or more trips to A&E. These may become relevant if it emerges that these trips correlate with police attendances at domestic disturbances.

**5.3** It is important that the information shared is relevant to the case and that neither too much nor too little detail is gone into. All information shared should be up to date and accurate.

## **6. Consent**

**6.1** It is best practice to obtain consent but is not obligatory in high risk cases as this approach is not always safe. It is recognised that there are circumstances where there is a need to share information without consent in order to protect an individual and/or any children. By sharing information to bring perpetrators to justice, as a matter of routine and good practice, agencies needing to share information should obtain explicit written consent or documented verbal consent from the victim of domestic violence. Such written consent should be retained on file with client correspondence in accordance with agency policy in relation to retention of information.

**6.2** CAADA have produced an Information Sharing without Consent form that should be completed where this is no consent (Appendix C) and retained on the client file in accordance with agency retention policy.

**6.3** If consent is refused, the referring agency then needs to consider whether risks to the victim justify the sharing of information, based on their best interests.

**6.4** Where personal information is shared without consent, full details need to be recorded about the information shared, the reasons justifying disclosure, the person authorising the disclosure and the person/agency with whom the information is being shared.

**6.5** In some situations it may be justified to share information without consent i.e. where there are risk factors involved such as safeguarding children are involved. Other examples might include:

- The prevention or detection of crime
- Significant harm
- Vital interests
- Medical harm
- Court order

**6.6** In some circumstances, consent should *not* be sought for example to do so would:

- Place a child at increased risk of significant harm
- Place an adult at risk of serious harm or
- Prejudice the prevention or detection of a serious crime
- Lead to unjustified delay in making enquiries about allegations of significant harm

**6.7** The perpetrator is unlikely to be informed about the meeting and the safety plans discussed as this would defeat the purpose of the safety plan. Participants should take extraordinary care not to inform the perpetrator of any element of the safety plan inadvertently.

## **7. Minimum Data Exchange**

### **7.1 MARAC Support Officer**

Referrals to MARAC will be made from various sources: Police, Refuge, IDVA, CRI and other agencies. The referral to MARAC will consist of a fully completed referral form together with a copy of the DASH Risk Assessment. Referrals made outside of Modus will be made electronically to the MARAC Support Officer to the following address:

Eastbourne, Wealden and Lewes MARAC

Email: [Eastbourne\\_Wealden\\_Lewes.MARAC@eastsussex.gov.uk.cjism.net](mailto:Eastbourne_Wealden_Lewes.MARAC@eastsussex.gov.uk.cjism.net)

Telephone: 01323 466549

Hastings and Rother MARAC

Email: [Hastings\\_Rother.MARAC@eastsussex.gov.uk.cjism.net](mailto:Hastings_Rother.MARAC@eastsussex.gov.uk.cjism.net)

Telephone: 01323 466549

Information provided to the group by the MARAC Support Officer will be recorded in the Modus case management system. The system is used for creating the meeting papers and case records.

**7.2** Information provided in advance of the meeting will include:

- MARAC Agenda – which will include all case names to be discussed at the MARAC
- Minutes of Previous Meetings – which will include all relevant information to each case previously discussed. Minutes will also record reasons for decisions to share, the extent of any disclosures made and the permitted use of the disclosed information
- MARAC Referral Forms – which contain appropriate information relevant to the referral.

**7.3** All information should where possible, be provided electronically, to a designated secure mail as standard. All attendees of MARAC must arrange access to secure mail services.

**7.4** In the case of agencies invited for the review of a specific case and only in exceptional circumstances, all documents must contain a password to open. The password should be mailed separately to the recipient.

**7.5** Where it is not possible to send the documents electronically, paper copies should be sent addressed to the identified recipient, by registered post and delivery confirmed by the recipient.

**7.6** There is a research form for agencies to use and to share relevant information held in relation to the victim, perpetrator and children. Key representatives will be expected to attend the MARAC to provide their expertise and present their research in the delivery of an action plan, regardless of involvement with an individual victim. The research forms will be completed in advance of the meeting and the information shared.

**7.7 Other Agencies/Organisations** are likely to provide the following information to those at the meeting:

- Name, date of birth, addresses, aliases and gender
- Current information relating to recent contact, meetings, sightings, phone calls which could include attendance or non-attendance at appointments, who is present at an address and attendance at A&E or other health setting
- Current information on attitude, demeanour, behaviour etc
- Information about Court Orders, injunctions, bail conditions and other legal issues
- Historic relevant information such as previous convictions, family or relationship history, other safety options considered or substance misuse issues
- Other information relating to the risks being faced by the victim or other data subjects
- Information about the suspected/known perpetrator
- Neighbourhood complaints
- Vandalism records.

The information likely to be shared by each agency attending the MARAC is summarised in the table:

**Table 1: Data Exchanged at MARAC**

Agency	Type of Data
Sussex Police	<ul style="list-style-type: none"> <li>• Number of previous Domestic Abuse Incidents/Offences relating to the offender and the victim</li> <li>• Relevant previous convictions from Police records</li> <li>• Details of incidents, use of weapons, threats to kill, threats to harm children, of any children present, living in the property or visiting or likely to be</li> <li>• Previous call outs to the address Breaches of bail</li> <li>• Any warning signals such as threats of suicide, drugs, alcohol, weapons, assault on police</li> </ul>
IDVA or other specialist support agency	<ul style="list-style-type: none"> <li>• Action/Safety Plan</li> <li>• Update on whether or not victim has engaged with the IDVA service</li> <li>• Update on whether victim has engaged with other agencies who might not be part of MARAC</li> <li>• Information about victim’s fears</li> </ul>

	<ul style="list-style-type: none"> <li>• Information about specific abusive behaviour</li> <li>• Details of impact on children</li> <li>• Actions taken by victim to protect themselves e.g. change phone number/ request for personal alarm</li> <li>• Information about harassment</li> <li>• Information about incidents not reported to the police</li> <li>• Update on other legal protection</li> <li>• Information about contact disputes</li> <li>• Victim needs to be re-housed</li> </ul>
Housing	<ul style="list-style-type: none"> <li>• Confirm information about incidents affecting property with dates</li> <li>• Information about where victim and perpetrator are living and terms of tenancy</li> <li>• If victim has made an application alone</li> <li>• Information about rent arrears</li> </ul>
Children and Young People's Services	<ul style="list-style-type: none"> <li>• Reason for referral</li> <li>• Feedback on assessment</li> <li>• Update on what support is in place and whether appointments are attended</li> <li>• Update on specific needs of children in need, children at risk and children with disabilities</li> </ul>
Health Visitor/ Midwife	<ul style="list-style-type: none"> <li>• Update on whether or not appointments are attended</li> <li>• Developmental update including progress of pregnancy, routine enquiry</li> <li>• Anything unusual about client e.g. attendance by partner at all appointments</li> <li>• Any damage noted to the home address on previous visits</li> </ul>
Probation	<ul style="list-style-type: none"> <li>• Previous history of convictions</li> <li>• Update on attendance at Integrated Domestic Abuse Programme (IDAP) / supervision</li> <li>• Breaches of orders</li> <li>• Update from Women's Safety Officer</li> <li>• Prison information such as recalls and release dates where possible</li> </ul>
Drug and Alcohol Treatment Providers	<ul style="list-style-type: none"> <li>• Perpetrator substance misuse issues</li> <li>• Victim substance misuse issues</li> </ul>
Adult Mental Health Teams	<ul style="list-style-type: none"> <li>• History of perpetrator mental health issues</li> <li>• History of victim mental health issues</li> </ul>
Refuge Providers	<ul style="list-style-type: none"> <li>• Previous stays in refuge with dates etc</li> <li>• Details of severity of abuse</li> <li>• Attempts by perpetrator to contact/ find victim</li> </ul>
A&E	<ul style="list-style-type: none"> <li>• Number of attendances with dates and pattern of injuries if possible for victim, perpetrator and children</li> </ul>
Adult Services	<ul style="list-style-type: none"> <li>• Update on specific needs of victim if a vulnerable adult</li> <li>• Update on needs/ services available to perpetrator if a vulnerable adult</li> </ul>
Education	<ul style="list-style-type: none"> <li>• School and attendance</li> </ul>

	<ul style="list-style-type: none"> <li>• School performance/ behavioural issues</li> <li>• Incidents at the school e.g. attempted abduction of child</li> <li>• Provide information on who takes and collects the child from school</li> </ul>
CAFCASS	<ul style="list-style-type: none"> <li>• Update on court proceedings and court orders</li> <li>• Feedback from supervised contact sessions</li> <li>• Views of children if appropriate</li> <li>• Professional opinion</li> <li>• History of involvement with either victim or perpetrator from previous cases, either public or private law</li> </ul>

### **7.8 Data Relating to Action Plans**

A number of risks will be identified relating to the victim, the perpetrator and the children and in some cases, staff or other individuals. It is helpful to reflect on these risks and to consider them in relation to the action plan. It is important that the information that is shared is relevant to the case and that neither too much nor too little detail is provided.

### **8. Data Relating to Perpetrators**

Data relating to suspected perpetrators and perpetrators will be captured by CRIDAS/IDVA and entered on to the Modus Case Management System - this includes:

- Name, date of birth and address
- Details of any distinguishing characteristics
- Name of any other known victim
- Details of any known perpetrator programmes attended

Information relating to perpetrators is shared at MARACs where appropriate.

#### **8.1 MAPPAs (Multi Agency Public Protection Arrangements)**

MAPPAs are the statutory arrangements imposing a duty to the Police, Probation and Prison Services for managing sexual, violent and terrorist offenders. MAPPAs are focused on the risk management of an offender but includes significant considerations with respect to associated victim issues relating to the offender.

**8.2** The MARAC Support Officer will share with the MAPPAs Co-ordinator the following information prior to the MARAC:

- MARAC Agenda

**8.3** Where the MAPPAs Co-ordinator has assessed that an offender may qualify as a MAPPAs offender, they will notify the MARAC Support Officer to that effect. Where a perpetrator is identified by the MAPPAs Co-ordinator as a MAPPAs offender, the following will be provided to the MAPPAs Co-ordinator:

- MARAC Risk assessment
- MARAC Referral

**8.4** Following the MARAC, further information will be shared:

- Minutes of the MARAC

**8.5** Where appropriate, the MARAC Support Officer will receive the MAPPAs minutes of meeting however this information will remain restricted and only a summary provided where appropriate to MARAC attendees.

## **9. Confidentiality**

**9.1** Consent of the victim, child or perpetrator should be sought in every case where possible but where there is no consent, decisions to disclose should be made on a case by case basis, based on the necessity to disclose, proportionate to the level of disclosure and all disclosures should be recorded. All disclosures of information should be carefully recorded at each MARAC meeting and records retained for a minimum period.

**9.2** CAADA provide guidance in relation to data sharing at MARAC meetings<sup>5</sup> and Appendix B contains the MARAC Confidentiality form that should be signed by all members of each meeting and retained by the MARAC Co-ordinator.

**9.3** Distribution of the Minutes of MARAC meetings should include the following statement: Those persons present were reminded that this meeting is strictly confidential. Discussions should not be shared outside of the meeting. Similarly, copies of the minutes should not be photocopied or shared without the agreement of the agencies concerned. All agencies should ensure that they develop procedures to ensure that the minutes are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to race, gender, sexuality and disability.

**9.4** Information shared at the MARAC is used to inform the Safety Plan that will address the risks faced by the adult victim and children. Decisions about how the information will be used should be made during the meeting,

CAADA guidance relating to frequently asked questions<sup>6</sup> includes:

- The perpetrator is not informed about the MARAC referral
- The case can be referred to another MARAC should the perpetrator move to a new area
- Information and reason to disclose might become apparent during the MARAC at which point, the information should be shared – the decision to disclose should be recorded

## **10. Recording Data**

**10.1** Data relating to victims and perpetrators of domestic violence will be recorded into the Modus Case Management System. The Modus system has an enhanced level of login security and active record restrictions. Security levels limit access to client records unless access has been specifically granted on an individual case basis. Systems administration and auditing processes will allow each individual access to specific areas within the system dependent upon their security access level. The system will enforce an audit trail regime, document all record edits and system access logs.

**10.2** Specifically named individuals at services/agencies who are likely to have access to the system include:

- Sussex Police
- Domestic Violence Provider
- Multi Agency Risk Assessment Conferences (MARACs) – MARAC officer
- Independent Domestic Violence Advisers (IDVA)
- Supporting People
- East Sussex County Council
- East Sussex Safer Communities Team

- Victim Support
- Specified community groups
- Children's Services

**10.3** The system allows for varying security levels to be set in order that those individuals with the necessary security level can access reports and information relating to their service and relating to their clients where appropriate. Data in the system is controlled and owned by the East Sussex Safer Communities Team.

All referrals to MARAC will be recorded in Modus, using the MARAC Referral form. Agendas and Minutes of MARAC meetings will be recorded in the system in addition to specific actions against individual victim/perpetrator records as agreed at the MARAC meetings.

## **11. Access and Security of Data**

**11.1** As the CJS Information Sharing Guidance suggests, agencies should ensure that security measures commensurate with the Data Protection Act 1998 that requires that:

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

In addition, agencies should 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 attached,  
Promote discretion in order to avoid unauthorised access.*

MARAC data is restricted and staff accessing information must be subject to the 'need to know' and to any specific additional restrictions agreed within agencies.

**11.2** The generic and secure email address for each MARAC:

- Eastbourne, Wealden and Lewes MARAC  
Email: [Eastbourne.Wealden.Lewes.MARAC@eastsussex.gov.uk.cjism.net](mailto:Eastbourne.Wealden.Lewes.MARAC@eastsussex.gov.uk.cjism.net)  
Telephone: 01323 466549
- Hastings and Rother MARAC  
Email: [Hastings.Rother.MARAC@eastsussex.gov.uk.cjism.net](mailto:Hastings.Rother.MARAC@eastsussex.gov.uk.cjism.net)  
Telephone: 01323 466549

**11.3** All emails relating to MARAC should be forwarded to the above email address via secure .cjism.net email. All mail sent to the MARAC address should be sent *from* a secure mail address to enable receipt of the mail.

Emails sent via the secure email system should not be forwarded to non-secure recipients.

## **12. Secure Storage of Data**

Data should be stored in accordance with the Data Protection principles in that:

- Data should be stored securely – only those who legitimately require access to the data should be allowed access

- Personal data processed for any purpose should not be kept longer than is necessary for that purpose
- The retention of data should comply with organisational policies

Steps should be taken by all Partners to ensure that information is securely stored and accessible by only those who are permitted access.

Where information is stored electronically, steps should be taken to ensure that files are created with restricted access to those permitted to access the data. Care should be taken when using electronic storage accessible to other individuals within own organisations.

### **13. Record Keeping of Data and Requests Outside of MARAC**

**13.1** As described in the CJS Guidance, all specific requests for information should be maintained securely and retained for a period appropriate to the agency and complexity of the information requested.

If the decision is to share, the information should be shared in the proper way, meaning that:

- The information shared is necessary for the purpose for which it is being shared
- The information is shared with the person or people who need to know
- That the information is accurate and up to date
- That it is shared securely
- That it is established whether the recipient intends or is allowed to share the information onwards
- That the data subject is informed that the data has been shared, if not already, where it is safe to do so

**13.2** It may be the case that where there is a genuine risk of crime to specific (named) individuals or a specific household, the Data Protection Act allows only the minimum necessary information to be disclosed by a MARAC agency to a non-MARAC recipient.

**13.3** It may be the case that in order to implement an effective safety plan for a victim, that persons who have not signed this guidance need to be informed of certain facts i.e. a perpetrator's name could be disclosed to a school so that the school knew not to admit the perpetrator to the premises. Another example could be where a perpetrator with convictions for violent behaviour moves to a neighbourhood and begins a relationship with a vulnerable woman or household. Information relating to the convictions could be disclosable between MARACs.

**13.4** Agencies receiving any information relating to MARAC are obliged to retain and use the information lawfully and the persons with whom the information is shared must know:

- Why they have been given the information i.e. the purpose for which the information has been given must be connected to that person's authority and role as a representative
- That the information must remain confidential, be kept and shared safely and securely and retained for as long as necessary and
- What they are expected to do with the information

#### **14. Process**

Agency protocols for disclosure requests should be followed and in normal circumstances, this would require any request to be made in writing. Requests for information under the Freedom of Information Act should be responded to within agency guidelines, allowing the MARAC Chair reasonable time for response. The MARAC Operating Protocol outlines processes at each stage of the MARAC.

#### **15. Disclosure Requests**

Such requests will always be made in writing and access limited to employees of MARAC members whose work is directly related to the aim for which the data was obtained and whose working within the crime reduction field. It is essential that when any disclosure is made, the person receiving the information is aware of the obligations this places on them and what they are able to do with the information.

#### **16. Subject Access Requests**

Data subjects are legally entitled to request their records from the receiving agency unless an exemption applies. Requests should be made in writing and processed by Designated Information Sharing Officers.

**17.** Requests for information under the Freedom of Information Act should be forwarded to the MARAC Chair who will make an informed decision based on the known facts and identified risks involved in the disclosure of the requested information.

#### **18. Weeding of Data**

MARAC members must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice.

#### **19. Media Involvement**

There should be a consistent approach to media enquiries and staff should not express personal views, respecting the requirement for confidentiality and discretions. Partners agencies agree to the development of a media strategy developed by the Safer Communities Team in partnership with the MARAC members. The strategy will ensure consistency, honesty, impartiality, and a consent-based approach when making information public.

#### **20. Information Sharing Complaints and Breaches**

**20.1** Any person/organisation wishing to make a complaint against another signatory agency about activities relating to information sharing or related issues at MARAC should in the first instance, submit the complaint in writing to the MARAC Chair who will refer such complaints to the MARAC Steering Group appropriately. An investigation of such a complaint will be undertaken in normal circumstances within two weeks.

- The MARAC Chair will investigate the complaint and inform MARAC partners of their response
- If necessary the MARAC Chair will take advice from the Data Registrar or their partners' organisations and from the Information Commissioner

- The result of the investigation shall be communicated in writing to the complainant and any redress made
- The MARAC Steering Group will review partnership and procedures in light of any complaint and make necessary changes

## **20.2 Breaches**

Any breaches of confidentiality and of the MARAC Operating Protocol will seriously increase the risk to a victim, affect the credibility of the MARAC and partnership objectives. All agencies must undertake at all times to comply with the data protection law and other legal requirements relating to confidentiality.

Any agency in breach will be subject to investigation by the MARAC Steering Group.

## **21. Agencies Agreeing to Abide By the Principles of the Guidance**

Signatories to the MARAC Operating Protocol (v5) have agreed to abide by the principles of the MARAC Information Sharing Guidance. The MOP and ISG will be reviewed at least annually and an index of signatories maintained by the MARAC Chair.

## Appendix A

# SUSSEX CRIMINAL JUSTICE BOARD

Criminal Justice System: working together for the public



## Multi–Agency

### Information Sharing Guidance

#### 1 INTRODUCTION AND PRINCIPLES OF THE GUIDANCE

- 1.1 Public sector agencies and organisations are able to make differing resource contributions to crime and disorder reduction. Information sharing between agencies is needed in order for various strategies to be successful, including tackling anti–social behaviour (ASB) and prolific and other priority offenders (PPOs) as well as the prevention, detection, investigation and prosecution of individual crimes. It also allows for specific activity relating to the Prevention of Violent Extremism.
- 1.2 In general terms, the law allows for information sharing for any legitimate purpose, where this has a legal basis.
- 1.3 There is a clear benefit in sharing data in order to protect the public and avoid individual tragedy that may follow when proper processes are not in place and communication is lacking.
- 1.4 The purpose of this guidance is to facilitate exchange of information between responsible agencies across Sussex for the purposes outlined in paragraph 1.1.
- 1.5 The scope of this guidance is to clarify the understanding between each agency / organisation’s responsibilities towards each other and data subjects.
- 1.6 The public rightly expect, and the Data Protection Act 1998 requires, that personal information held by statutory agencies will be properly protected. However, there is also a public expectation that there will be an appropriate sharing of information in working in partnership towards reducing crime and disorder and protecting public health.
- 1.7 Section 115 of the Crime and Disorder Act 1998 gives “power”, but not an automatic right, to disclose information.
  - (1) Any person who, apart from this subsection, would not have power to disclose information—
    - (a) to a relevant authority; or
    - (b) to a person acting on behalf of such an authority,shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.
  - (2) In subsection (1) above, “relevant authority” means—
    - (a) the Chief Officer of police for a police area in England and Wales;
    - (b) the Chief Constable of a police force maintained under the [1967 c. 77.] Police (Scotland) Act 1967;
    - (c) a police authority within the meaning given by section 101(1) of the [1996 c. 16.] Police Act 1996;

(d) a local authority, that is to say—

(i) in relation to England, a county council, a district council, a London borough council or the Common Council of the City of London;

(ii) in relation to Wales, a county council or a county borough council;

(iii) in relation to Scotland, a council constituted under section 2 of the [1994 c. 39.] Local Government etc. (Scotland) Act 1994;

(e) a probation committee in England and Wales;

(f) a health authority.<sup>1</sup>

- 1.8 Although not mandatory, Section 115 provides the lawful power for anyone to disclose information to a relevant authority – i.e. the police, police authority, local authority, probation committee or health authority, or to any persons acting on their behalf - where this is necessary or expedient for the purposes of a provision of the Act.
- 1.9 Section 115 does not, however, override the need to disclose in a proper manner, taking into account other statutory and common law constraints on disclosure, including data protection, human rights and the common law duty of confidence. These are set out in more detail for reference at Annexes 1 to 3 and will be applied and followed by all organisations in implementing this guidance.
- 1.10 It is important to put in place sound arrangements for information sharing, so as to be clear about the processes involved and the type of information to be shared, and to ensure compliance with Data Protection legislation.
- 1.11 The data protection principles require that information is obtained and processed fairly and lawfully; is only disclosed in appropriate circumstances; is accurate, relevant and not excessive; not held longer than necessary and is kept securely.
- 1.12 Whilst therefore, consent of the individual is not always required in the public interest<sup>2</sup>, obtaining consent remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought from and freely given by the data subject.
- 1.13 The agency receiving data will not use it for any purpose other than that set out in this guidance, nor share it with any other party, without the disclosing partner's explicate permission.
- 1.14 Each agency/organisation undertakes to ensure that it complies with all relevant legislation, common law duties, and its own internal policies and procedures on disclosure, as well as the guidance and practice contained in this guidance.

## 2 DATA

This section sets out the different forms of data that may be shared.

### 2.1 Non-personal data

- Non-personal data is data that *does not, nor has ever, referred to individuals*. The Data Protection Act places no restrictions on the disclosure of information which does not identify individuals. If non-personalised data can be used for information sharing

---

<sup>1</sup> reference Crime and Disorder Act 1998 C.37,Part V, S115- disclosure of information

<sup>2</sup> in circumstances where information sharing is needed for;-

- administration of justice
- maintaining public safety
- apprehension of offenders
- prevention and crime, disorder and violent extremism
- detection of crime
- protection and intervention of vulnerable members of the community

purposes, there will be no data protection implications. Disclosure shall be limited to non-personalised data wherever possible.

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

## 2.2 Depersonalised data

- Depersonalised data encompasses any information that *does not and cannot be used to establish the identity of a living person, having had all identifiers removed*. All participants in this protocol must recognise that great care must be taken when depersonalising data; even a post-code or address can reveal the identity of an individual. Organisations need to be aware that it may be possible for an individual's identity to be revealed by comparing several sets of depersonalised data.
- There are no restrictions under the Data Protection Act 1998 on the exchange of depersonalised data, although a duty of confidence may apply in certain circumstances, or a copyright, contractual or other legal restriction may prevent the information being disclosed to partners. This is to be decided on a case by case basis by the disclosing organisation.

## 2.3 Personalised data

- Personal data (to be considered separately from *sensitive* personal data at 2.4) is information that relates to a living individual who can be identified from that data or from those data and other data in the possession of the data controller and includes expression of opinion or intentions towards the data subject.
- Consent of that data subject will accompany the exchange request or there will be an *overriding* public interest e.g., to prevent or detect crime (where there is no consent).
- Any disclosure of personal information must have regard to both common and statute law, for example defamation, the common law duty of confidence and the Data Protection principles. Participating agencies will also be subject to their own policies and guidance on information exchange.
- Only sufficient information will be disclosed to enable partners to carry out the relevant purpose for which the data is required. This will be determined on a case by case basis, through negotiation between disclosing and receiving partners where necessary.
- Each agency/organisation will keep a record of all requests to and from other agencies/organisations to this guidance for personal information. Any request will clearly set out the purpose or purposes for which the information is requested. It will also specify as clearly as possible how failure to disclose such information would prejudice this purpose.
- The data owner will carefully consider the relevance of the information being requested and shall make a record of the factors taken into consideration in reaching their decision. Steps will be taken to ensure the security of such information by the agencies handling and sharing such information and undertake to destroy all personal data when no longer required for the purpose for which it was provided.
- At least one condition of Schedule 2 of the Data protection Act 1998 will be satisfied where it is necessary to process personal data, as set out in **Annex 4**.

## 2.4 Sensitive personal data

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

- i. Racial or ethnic origin
  - ii. Political opinions
  - iii. Religious beliefs or other beliefs of a similar nature
  - iv. Trade union membership
  - v. Physical or mental health or condition
  - vi. Sexual life
  - vii. Commission or alleged commission of any offence
  - viii. Any proceedings for any offence committed, or alleged to have been committed.
- Any disclosure of sensitive information by a partner should be restricted to the minimum necessary to achieve the purpose and be as generalised as possible.
  - Participating agencies and organisations must ensure that at least one condition of schedule 2 *and* at least one condition *of* schedule 3 of the Data Protection Act 1998 are satisfied where it is necessary to process sensitive data at point of disclosure as set out in **Annex 5**.

### 3 **PRINCIPLES TO BE APPLIED IN SHARING DATA**

- 3.1 Many of the data protection issues surrounding disclosures can be avoided if the consent of the individual concerned has been sought and obtained. Obtaining the consent of the individual concerned or other relevant individual must always be considered and details of arguments for and against obtaining that consent must be fully documented.
- 3.2 The organisations to this guidance will determine locally the procedures for disclosure subject to paragraph 4 below.
- 3.3 To ensure that a fair balance is achieved between the protection of the individual's rights and the general interests of society, the disclosing agency will consider whether any disclosure is proportionate and the decision as to whether disclosure will be made remains with the disclosing agency.
- 3.4 To enable the requesting agency and organisations to make the most informed, considered and effective decisions regarding the appropriate course of action in any specific case, information will need to be exchanged at the earliest possible opportunity.
- 3.5 Requests (for personalised data) should follow a consistent and carefully recorded format including:-
- The date that the request was made;
  - The name of the individual about whom the information is requested;
  - Other identifying information as appropriate i.e. date of birth, address, sex;
  - Racial origin of the individual if appropriate;
  - The purpose for which the information is required;
  - Why the information is necessary for that purpose, e.g. proceedings may fail without the information/ the crime reduction initiative would be jeopardised;
  - Explanation of what the assumed successful effect upon the case would be if disclosure is made;
  - A clause stating that the information will only be used for that purpose;
  - The name of the person requesting the information;
  - The designation of the person requesting the information;

- The address (including secure e-mail where it exists between partner agencies but not facsimile) for responding to the request.
- 3.6 Extreme care needs to be taken to ensure that innocent victims, witnesses, or complainants are never identified. This is particularly important in cases of Domestic Violence, Serious Sexual assault and Honour Based Violence due to the unique relationship between the victim and perpetrator and/or where children are involved.
  - 3.7 Details of cautions (or reprimands/warnings issued under the Crime and Disorder Act 1998) which relate to an adult will not generally be disclosed, as the cautioning procedure creates an expectation that the offence has been dealt with and that no further action will be taken.
  - 3.8 Where information is sought by or from any health service or practitioner, regard will be had to the NHS Code of Practice on Confidentiality (November 2003), relevant health legislation<sup>3</sup> and any current relevant health services protocol in place across Sussex.
  - 3.9 Information provided will be retained no longer than is necessary to achieve the specific objective and will then be destroyed. Data will be weeded and a maximum retention period for data agreed between partner agencies.
  - 3.10 The organisations shall have designated officers to deal with information exchange and there will be a minimum number of designated officers in order to retain confidentiality and operational effectiveness, dependent on the size and structure of the specific organisation. Such designated officers shall have received appropriate training on the provisions of the Data Protection Act 1998.
  - 3.12 A secure administration system should be designed and implemented which will prevent unauthorised access to and disclosure of personal or sensitive personal data.

#### 4 DESIGNATED OFFICERS

- 4.1 In order to ensure compliance with the Data Protection Act, the parties to this guidance shall nominate one or more designated officers to whom all requests and from whom all disclosures of personal information will be made.
- 4.2 It will be the responsibility of each agency to ensure that their designated officers are trained in and fully conversant with the requirements of the Data Protection Act 1988.
- 4.3 It is the responsibility of these officers to ensure that all relevant legal requirements are observed.
- 4.4 The parties to this guidance will maintain and update a list of designated officers, notified to all parties.
- 4.5 Primary responsibilities of designated officers, who are the primary data owners for their agency, will include ensuring:-
  - compliance with this guidance by their agency;
  - processing of personal data is in accordance with the principles of the Data Protection Act 1998<sup>4</sup> and as laid down in **Annexes 1 & 3**;

---

<sup>3</sup> E.g. regarding sexually transmitted diseases, human fertilisation and embryology and Data Protection (Subject Access) (Health) Order

<sup>4</sup> Data Protection Principles

- Processed fairly and lawfully
- Obtained for only one or more specific and lawful purpose
- Adequate, relevant and not excessive
- Accurate and where necessary kept up to date

- formal requests for information are made only through them;
- they determine, either alone or, where appropriate, in consultation with other members of their agency/organisation, the question of disclosure;
- regular periodic review of material held or disclosed, including correcting inaccuracies, and its destruction;
- administration of records, including minutes of decisions reached at meetings;
- managing and determining individuals' rights of access to personally identifiable information held about them.

## 5 ACCESS BY OTHERS

- 5.1 The data subject is legally entitled to request their records from the receiving agency under Section 7 of the Data Protection Act 1998, unless an exemption applies. If a subject requests access to their records, the receiving agency should contact the disclosing agency to determine whether the latter wishes to consent to the disclosure or claim any exemption.
- 5.2 Care will be taken when handling the media to ensure that:
- there is a consistent and agreed approach to media enquiries between all organisations in this guidance;
  - information provided into the public arena will be fair and honest, balance the rights of the individual and the public interest and maintain integrity between the partner agencies;
  - where an individual may be identified, that person is consulted in advance where practical;
  - personal information disclosed to a partner agency is not released to the media without prior consultation with that agency;

An agreed media strategy may be referred to by partner organisations. This would be in compliance with any SCJB strategy.

- 5.3 Access to information by others in the partner agencies apart from the designated officers should be limited to that which is necessary for the aim/purpose for which the information is being disclosed and agreed with the disclosing agency.
- 5.4 Further disclosure of personal data to any other agency or organisation will require the consent of the data subject or the designated officer for the disclosing party, who will need to weigh confidentiality and the public interest in disclosure. Common law protects from disclosure information, (whether personal or not), that is given in circumstances giving rise to an obligation of confidence on the part of the person to whom the information has been given. All health information is subject to this duty of confidence.

## 6 SECURITY OF DATA

- 6.1 Security arrangements will be put in place by the agencies/ organisations to this guidance to protect the integrity and confidentiality of the information held.
- 6.2 Such arrangements should include a secure environment and inputting systems in which:-
- e-mail communication over internet links is avoided;
  - there is back-up protection;

- 
- Not kept longer than is necessary
  - Processed in accordance with the rights of the data subject
  - Kept securely
  - Not transferred outside of the EAA unless adequate protection

- there is password protection for material on computer systems;
- paper information is kept in securable storage, with restricted, authorised access.
- Disposal of information must be in accordance with each organisation's retention policies.

## **7 COMPLAINTS AND BREACHES**

- 7.1 Any formal complaint by a data subject regarding any stage of the process should be notified in writing to all the agencies and organisations involved. They will do all they can within the guidelines of the Data Protection Act 1998 to assist with a complaint under the usual complaint procedures for their agency.
- 7.2 All agencies will undertake to comply with all data protection, human rights, common law and other legal requirements with regard to confidentiality.
- 7.3 In the event of a breach by any of the signatory agencies and/or organisations of this guidance, as receivers of information, will accept total liability for any breach of this information sharing guidance, should legal proceedings be served in relation to the breach.

## **8 AGENCIES/ORGANISATIONS USING THIS GUIDANCE**

- 8.1 The agencies/organisations using this guidance should agree:-
- to subscribe to the principles contained in this guidance;
  - to work to the procedures identified within the guidance;
  - to implement the guidance fully within their own agency, ensuring staff support and attendance at any appropriate training event;
  - Supply information to other agencies/organisations at no financial cost;
  - to contribute to the development of trust and confidence between the participating agencies by working within the framework of the guidance and to promote public health and safety, prevention of crime and disorder and the protection of rights and freedoms.
- 8.2 Chief Officers recognise that this guidance is subject to an annual review.

## **ANNEX 1**

### THE DATA PROTECTION PRINCIPLES

#### *The First Principle*

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- (a) at least one of the conditions in Schedule 2 is met; and
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is met.

#### *The Second Principle*

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

#### *The Third Principle*

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

#### *The Fourth Principle*

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

#### *The Fifth Principle*

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

#### *The Sixth Principle*

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

#### *The Seventh Principle*

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

#### *The Eighth Principle*

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

## **ANNEX 2**

### **HUMAN RIGHTS ACT 1998**

Article 8 of the European Convention on Human Rights states that everyone has the right to respect for his private and family life, home, and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of:

- i. National security;
- ii. Public security;
- iii. Economic well being of the country;
- iv. The prevention of crime and disorder;
- v. The protection of health or morals;
- vi. The protection of the rights or freedoms of others.

Current understanding is that compliance with the Data Protection Act 1998 and the common law duty of confidentiality should satisfy Human Rights requirements.

In order to ensure that a fair balance is achieved between the protection of the individual's rights and the general interests of society, the Convention therefore requires the disclosing agency to consider whether any disclosure is proportionate.

## **ANNEX 3**

### **COMMON LAW DUTY OF CONFIDENCE**

The common law principle is that where information is given in circumstances where the recipient has an obligation of confidence, this information should not be further disclosed, except as agreed with the confider.

However, this is not an absolute bar to disclosure where the public interest indicates that to be appropriate.

This means that in any given case, the person who has the information must make a judgment as to the strength of the public interest in overriding the duty of confidence. The case of **Mc Cann [2002] UKHL 39**, a case dealing with anti-social behaviour, laid down the principle that the striking of a fair balance between the general interests of the community and the protection of defendants' rights required that the scales came down in favour of community protection.

Confidentiality can also be overridden or set aside by legislation.

## **ANNEX 4**

### **SCHEDULE 2 DATA PROTECTION ACT 1998**

Schedule 2 reflects the requirement to make data processing legitimate. At least one condition must be met before any processing of the data can take place. The conditions are:

1. That the data subject has given his consent to the processing
2. That the processing is necessary:
  - for the performance of a contract to which the data subject is a party, or
  - for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary:
  - for the administration of justice,
  - for the exercise of any functions conferred on any person by or under any enactment,
  - for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
  - for the exercise of any other functions of a public nature exercised in the public interest by any person.
6. (1) the processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.  
(2) The Secretary of State may by order specify particular circumstances in which this condition is or is not to be taken to be satisfied .

## **ANNEX 5**

### **SCHEDULE 3 DATA PROTECTION ACT 1998**

At least one condition of Schedule 3 must be met before any information classed as 'sensitive personal data' may be fairly and lawfully processed. The conditions are:

1. That the data subject has given his explicit consent\* to the processing of the personal data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.  
(2) The Secretary of State may, by order: –
  - (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
  - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
- 3 The processing is necessary -

- (a) in order to protect the vital interests of the data subject or another person, in any case where -
    - (i) consent cannot be given by or on behalf of the data subject, or
    - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
  - (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
- 4 The processing -
- (a) is carried out in the course of its legitimate activities by any body or association which -
    - (i) is not established or conducted for profit, and
    - (ii) exists for political, philosophical, religious or trade union purposes;
  - (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
  - (c) relates only to individuals who, either are members of the body or association, or have regular contact with it in connection with its purposes, and
  - (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
- 5 The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
- 6 The processing -
- (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
  - (b) is necessary for the purpose of obtaining legal advice, or
  - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
- 7 (1) The processing is necessary -
- (a) for the administration of justice
  - (b) for the exercise of any functions conferred on any person by or under an enactment, or
  - (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
- (2) The Secretary of State may, by order -
- a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
  - (b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
- 8 (1) The processing is necessary for medical purposes and is undertaken by -
- (a) a health professional, or
  - (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
- (2) In this paragraph 'medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services.
- 9 (1) The processing -

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,  
(b) is necessary for the purpose of identifying, or keeping under review, the existence of absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained.

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

- Explicit Consent should be taken to mean that the data subject is fully informed about what they are consenting to. Ideally this consent should be documented within the record. It should be noted that consent can be withdrawn at any time

## ANNEX 6

### SEVEN GOLDEN RULES FOR INFORMATION SHARING.

The seven golden rules, along with the flow chart questions, will assist and support individuals decision making allowing confidence that information is being shared legally and professionally.

**1. Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately.

**2. Be open and honest** with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

**3. Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

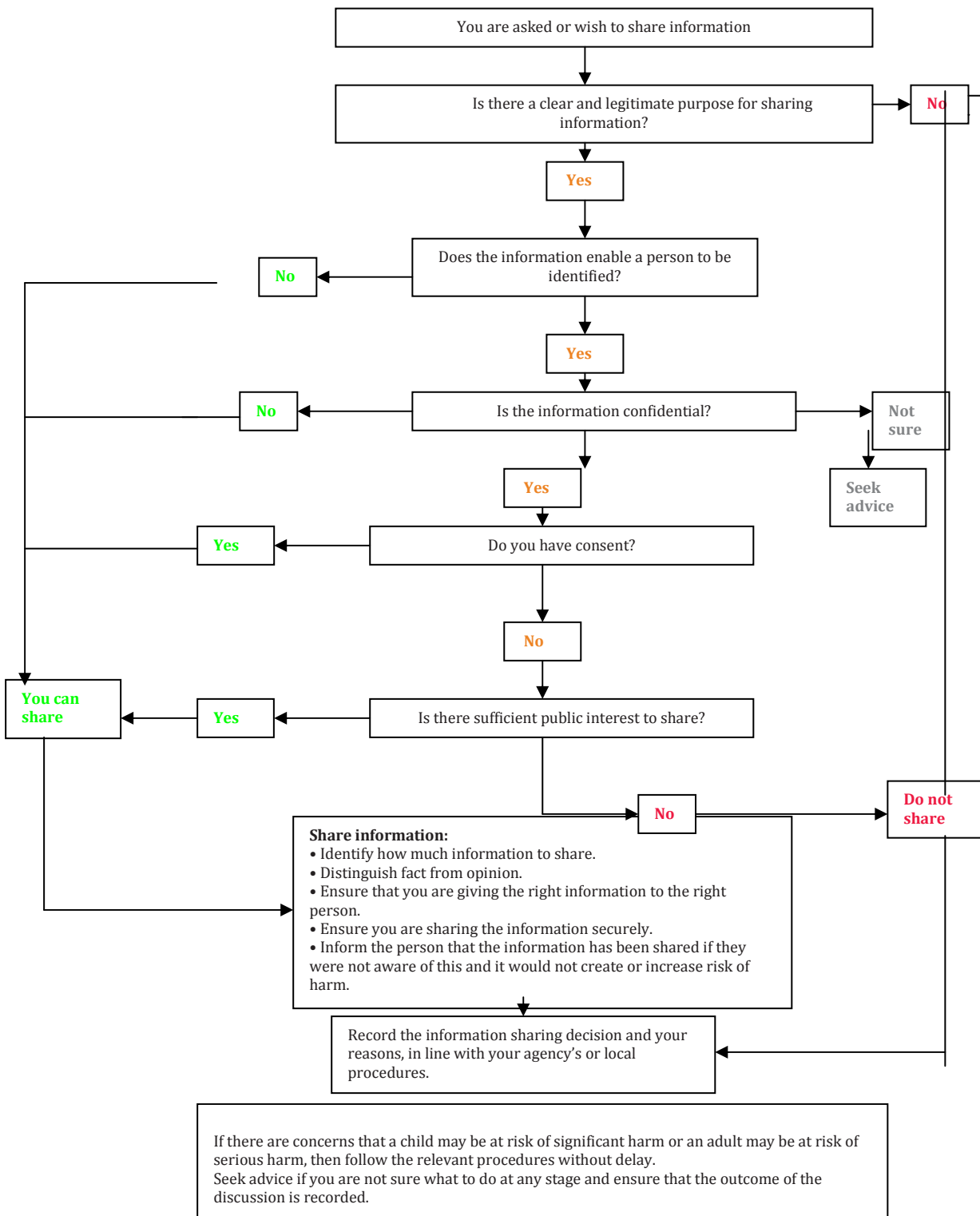
**4. Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.

**5. Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

**6. Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

**7. Keep a record** of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

## FLOW CHART OF KEY QUESTIONS FOR INFORMATION SHARING.



Taken from Information Sharing: Pocket Guide, HM Government information sharing guidance package (2008).

## ANNEX 7

### Example Form: Request for Personal Information

<b>Application protocol of</b>	Applies to requests regarding Prison Inmate location for the purpose of facilitating either a) a production order request by Police or, b) other specified reason.
<b>Process</b>	
	<ol style="list-style-type: none"> <li>1. Prisoner location information sought by Police to enable a production order request for the prisoner or for other specified reason.</li> <li>2. Police apply to Prisoner Location Service, (PSL) for location details of the prison inmate via Secure E-mail using the relevant form.</li> <li>3. The content of the subject line is particularly important to the PSL. Ensure the requirements in the subject line box are followed.</li> <li>4. Prison confirm location of inmate to Police by completing and returning form received from Police.</li> </ol>
<b>Form</b>	Pre prepared form ' <a href="#">Prisoner Location Request</a> ' located in Templates is to be used
<b>Hard Copies</b>	<ol style="list-style-type: none"> <li>1. Police will not create a hard copy.</li> </ol>
<b>Contingency</b>	
Local systems problems.	<ol style="list-style-type: none"> <li>1. Revert to fax 0121 626 3474.</li> </ol>
<b>Deleting/removing items.</b>	
When	As soon as the need to retain the information has ceased.
<b>Legal Issues</b>	
Target location	<a href="mailto:Prisoner.location.service@hmps.gsi.gov.uk">Prisoner.location.service@hmps.gsi.gov.uk</a> No suffix is required as the e-mail is between agencies both of whom are within the secure e-mail environment.
Checking currency	The mail box will be checked by HMPS throughout the day between 0800 – 1600 Mon to Fri. (Not Bank Holidays).
Status	<u>Urgent if:</u> <ol style="list-style-type: none"> <li>1. Next court appearance within 10 working days.</li> <li>2. Enquiries into Murder, Manslaughter, Sexual Offences, Child Protection and Domestic Violence Issues.</li> </ol> <u>Non Urgent if:</u> <ol style="list-style-type: none"> <li>1. Not within the above criteria.</li> </ol>
Response time.	The response will be: <ol style="list-style-type: none"> <li>1. Working Day for Urgent Requests</li> <li>2. working days for Non Urgent requests.</li> </ol>
Handling Documents	<ol style="list-style-type: none"> <li>1. Police will save a copy of the Prisoner Location Request form in 'Prison Requests and responses' folder under the name of the defendant, until location confirmed.</li> </ol>

To whom the reply is sent	Relevant e-mail address chosen from drop down box on form in 'E-mail address for HMPS reply' field.
<b>Security</b>	
Address status	The information is within 'Restricted Status'.
General	It is the responsibility of the sender to ensure the secure address is used when personal details are sent. Failure must be reported as a security breach.
Subject Line	The subject line must not contain any restricted information as it is not encrypted but must inform the receiver if the enquiry is urgent and if for a court appearance the court venue. e.g. ' <b>Urgent/Non Urgent Hastings MC.</b> '  No reference will be made to the name of the defendant or anything that may lead to identification of the defendant.

## GLOSSARY

**Single Point of Contact (SPOC)** - a person or a department serving as the co-ordinator or focal point of information concerning an activity or program.

**Restricted** – The compromise of this material would be likely to:

- Cause substantial distress to individuals
- Prejudice the investigation or facilitate the commission of crime
- Breach proper undertakings to maintain the confidence of information provided by third parties
- Breach statutory restrictions on disclosure of information(e.g. unauthorised disclosure of personal data contrary to the Data Protection Act).
- Disadvantage Sussex Police in commercial or policy negotiations with others.

**Confidential** - The compromise of this material would likely to:

- Prejudice individual security or liberty
- Cause damage to the operational effectiveness or security or intelligence operations
- Impede the investigation or facilitate the commission of serious crime

**Secret** - The compromise of this material would likely to:

- Threaten life directly or seriously prejudice public order or individual security or liberty
- Cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations

**Top-Secret** - The compromise of material would likely to:

- Lead directly to widespread loss of life

- Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations

**Anti-Social Behaviour (ASB)** - is any aggressive, intimidating or destructive activity that damages or destroys another person's quality of life.

**Prolific and Other Priority Offenders (PPOs)** - offenders who commit a high volume of crime. The PPO programme is composed of three complementary strands: **Prevent and Deter, Catch and Bring to Justice, Resettle and Rehabilitate.**

**Disclosure** – the act or process of revealing or uncovering.

**Data Controller** - a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data are, or are to be, processed.

**Non-personal Data** – data that does not, nor has ever, referred to individuals.

**Depersonalised Data** – are individual records from which some of the personally identifiable fields have been removed. These fields include, but are not limited to: name, address and telephone number.

**Personal Data** – means data which is relate to a living individual who can be identified:

- From those data or
- From those data and other information which is in the possession of or is likely to come in the possession of the data controller

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

**Sensitive Personal Data** - data which relates to the data subject's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence
- Any proceedings for any offence committed, or alleged to have been committed.

**Appendix B**

**MARAC CONFIDENTIALITY DECLARATION**

**CONFIDENTIALITY DECLARATION**

**DATE:** .....

**THE CHAIR OF THE MEETING REMINDS ALL CONCERNED OF THE PROTOCOLS WITHIN THE AGREED DOMESTIC ABUSE SHARING OF INFORMATION DOCUMENT:-**

INFORMATION DISCUSSED BY THE AGENCY REPRESENTATIVE, WITHIN THE AMBIT OF THE MEETING IS STRICTLY CONFIDENTIAL AND MUST NOT BE DISCLOSED TO THIRD PARTIES WHO HAVE NOT SIGNED UP TO THE 'DOMESTIC ABUSE INFORMATION SHARING PROTOCOL' WITHOUT THE AGREEMENT OF THE PARTNERS OF THE MEETING. **This does NOT preclude any attending professional from 'flagging and tagging' MARAC subjects on their own agency's records so that all other colleagues who may have cause to deal with a MARAC victim, their children or the perpetrator, are alerted to their MARAC status and thus their high risk levels.**

IT SHOULD FOCUS ON DOMESTIC VIOLENCE AND CHILD PROTECTION CONCERNS AND A CLEAR DISTINCTION SHOULD BE MADE BETWEEN FACT AND OPINION **AND ALL INFORMATION SOURCED TO A NAMED INDIVIDUAL..**

ALL AGENCIES SHOULD ENSURE THAT THE MINUTES ARE RETAINED IN A CONFIDENTIAL AND APPROPRIATELY RESTRICTED MANNER. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to race, gender, sexuality and disability.

**THE PURPOSE OF THE MEETING IS AS FOLLOWS:**

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



**Appendix C  
Information-Sharing without Consent Form**

**Client information**

**Date:** \_\_\_\_\_

<p><b>Name/address of client:</b></p> <p><b>Names and D.O.B. of children:</b></p>
--

**Safety Concerns**

<b>Risk identified</b>	Immediate risk/crisis	Ongoing risk identified:	
		Risk assessment	Professional judgment
Danger to client	c	c	
Child(ren) at risk/Danger to child(ren)	c		c
Client poses a risk to self or others	c		c

**Check that consent form does not cover this situation &/or you do not have consent.**

**Risk Assessment** \_\_\_\_\_ (No. of ticks out of 20)  
(You may have the opportunity to complete a formal RA in an emergency. If you have, please attach it.)

**Details of incident/information causing concern:** (include source of information)

**Legal Authority to Share**

<p><b>c Local protocol relevant</b> _____</p> <p><b>OR</b></p> <p><b>Legal grounds</b> (please tick relevant grounds)</p> <p><b>c</b> Prevention/detection or crime and/or apprehension or prosecution of offenders (DPA, s. 29)</p> <p><b>c</b> To protect vital interests of the data subject; serious harm or matter of life or death (DPS, Sch. 2 &amp; 3)</p> <p><b>c</b> For the administration of justice (usually bringing perpetrators to justice (DPA, Sch. 2 &amp; 3)</p> <p><b>c</b> For the exercise of functions conferred on any person by or under any enactment (police/social services) (DPA, Sch. 2 &amp; 3)</p>
---

- c In accordance with a Court order
- c Overriding public interest (Common law)
- c Child protection – disclosure to social services or police for the exercise of functions under the Children Act, where the public interest in safeguarding the child’s welfare overrides the need to keep the confidential information (DPA, Sch. 2 & 3)
- c Right to life (Human Rights Act, Art. 2)
- c Right to be free from torture or inhuman or degrading treatment or punishment (Human Rights Act, Art.3)

**If you have legal authority to share, consider the following:**

**Balancing Considerations**

These could tip the decision to disclose either way:

- c Pressing need
- c Respective risks to those affected
- c Interest of other agency/person in receiving it
- c Public interest in disclosure
- c Human rights of client (Art 8 – right to a private life)
- c Duty of confidentiality

**Which of the above were compelling in your decision to disclose, or not disclose:**

**Internal consultations:** (Names, dates and advice/decisions)

**External consultations:** (Home Office guidance, Information-Sharing Helpline)

**Client notification**

<b>Client notified of disclosure(s)? Yes/No</b>	<b>Date:</b>
<b>If not, why not?</b>	

**Review**

<b>Date for review of this situation:</b> _____ (Review to include feedback from the agencies informed as to their response.)
_____
(Name)
<b>is responsible for ensuring the situation is reviewed by this date.</b>

**Record following details of information-sharing in case file:**

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

\_\_\_\_\_  
**Signed & dated by Caseworker**

\_\_\_\_\_  
**Signed and dated by Manager**

---

<sup>1</sup> Sussex MAPPA (multi-agency public protection arrangements) & MARAC Protocol (V1.5) available from [www.safeomeastsisse.org.uk](http://www.safeomeastsisse.org.uk)

<sup>2</sup> Sussex Wide Information Sharing Agreement available at:  
<http://drugs.homeoffice.gov.uk/publication-search/dip/sussex-cri-info-share-protocol?view=Binary>  
(Accessed 13/5/09)

<sup>3</sup> CJS Information Sharing Guidance – unpublished but available from Safer Communities Team:  
[www.safeineastsussex.org.uk](http://www.safeineastsussex.org.uk)

<sup>4</sup> CAADA MARAC Implementation Guide December 2007 available at:  
<http://www.caada.org.uk/searchresult.html?sw=information%20sharing>  
(Accessed 2/1/09)

<sup>5</sup> CAADA, Disclosure of Information During and After MARAC Meetings, FAQs available at:  
[www.caada.org.uk/searchresult.html?](http://www.caada.org.uk/searchresult.html?)

<sup>6</sup> CAADA *Disclosure of Information During and After MARAC Meetings: Frequently Asked Questions*  
Available at:  
[http://www.caada.org.uk/practitioner\\_resources/Disclosure\\_of\\_Info\\_at\\_MARAC\\_FAQs.pdf](http://www.caada.org.uk/practitioner_resources/Disclosure_of_Info_at_MARAC_FAQs.pdf)  
(accessed 10/1/10)