Data/Information Sharing Agreement – Domestic Abuse Multi-Agency Risk Assessment Conference (DA MARAC)

Contents

1. Introduction to the Sharing

The Domestic Abuse MARAC (Multi-Agency Risk Assessment Conference) aims to review and co-ordinate service provision in high-risk domestic abuse cases. The MARAC facilitates, monitors and evaluates effective information sharing to enable appropriate actions to be taken to increase public safety. This Data Sharing Agreement [DSA] documents how the parties to this agreement will share personal data to allow the parties to support and protect victims of domestic abuse (DA) at high risk of harm.

The parties agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Outline the Personal, Special Category and Criminal Data to be shared.
- Set out the lawful basis condition under UK GDPR (UK General Data Protection Regulation) and Data Protection Act 2018 through which the information is shared, including law enforcement processing and reference to the Human Rights Act 1998 and the Common Law Duty of Confidentiality.
- Stipulate the roles and procedure that will support the processing/sharing of information between agencies.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

Parties to this agreement cannot amend or add appendices unless agreed as part of a formal review. It is expected that each party will have procedures, processes and policies sitting underneath this agreement, for their respective organisations. These will, for example, describe the specific processes for secure transfer of data.

1.1. Ownership of this agreement

This agreement was drafted by a working group of representatives of the parties. These professionals were specialists in safeguarding, social work, police procedures, information governance and law. The local authority representatives worked under the banner of the Information Governance for London Group (IGfL), to draft one agreement that would work for all boroughs, CCGs (Clinical Commissioning Groups) and police BCUs (Borough Command Units) across London, as well as other partners. The aim is to reduce the number of versions of sharing agreements that historically differed between boroughs, partly to reduce the burden on pan-London organisations, that must have agreements with multiple boroughs.

IGfL, a group of information and security professionals at London boroughs, assisted with co-ordination of this agreement, but the responsibilities within it, and compliance with data protection legislation, remain with the data controllers that are party to this agreement.

1.2. Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act. Signatories are identified as those who have signed this agreement on the platform on which this agreement is hosted.

All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights & complaints, identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality, and seek advice from the relevant Data Protection Officer when necessary.
- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ, and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

The parties recognise that any one of them may share data with non-core agencies where relevant to the individual case. These organisations may attend MARAC meetings

Non core agencies

- Other VAWG (Violence Against Women and Girls) support services
- Housing Associations

- Other Health Services
- Sanctuary schemes
- Other Voluntary Agencies
- Other Non-Core Agencies may be identified and approved by the MARAC Chairs.

These organisations may be contracted by the core partners to deliver services such as victim support and refuges. These organisations are usually considered data controllers in their own right when delivering this contracted work, due to their independence and professional responsibilities.

Guest Agencies

Other agencies may be invited to attend or supply information to the MARAC to provide relevant information on a case and assist in the development and execution of the risk management plan. These will be guest agencies to the MARAC and can attend if invited. Guest agencies only attend for the case discussion of the specific case(s) they are attending for and only receive the relevant minutes and actions.

Organisations and their staff must consult the organisation's Data Protection Officer/Information Governance Lead and/or Caldicott Guardian if they are unsure at any point in the processing and sharing of personal data.

1.3. Confidentiality and vetting

Each party must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality.

Each party must ensure that suitable vetting has taken place. For some organisations this will be through standard employee checks (Baseline Personnel Security Standard or equivalent), but may be Disclosure & Barring Service (DBS), or Security Vetting (SV) or similar.

1.4. Assessment and review

A review of this information sharing agreement will take place every two years, unless otherwise agreed by the organisations' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not slipped, the benefits to the data subjects and organisations are being realised, and the procedures followed for information security are effective.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise, as will any changes to the signatory parties.

The working group who drafted this agreement strongly recommend that a working group approach is used for any reviews, as this was a successful way to achieve pan-London and cross-specialism consensus to one sharing agreement.

1.5. Termination of agreement

In the event of termination of this agreement each party may continue to hold information originating from other parties, for which they are Data Controller.

2. Purpose and Benefits

There is multiple legislation that covers the work of managing and reducing domestic abuse.

ACPO Definition of "domestic abuse"

The DA Act gained Royal Assent on 29th April 2021, however there are several elements NOT yet in force. The MPS awaits guidance from NPCC and College of Policing as the changes come into effect.

Until such time the MPS follows CoP APP
https://www.app.college.police.uk/app-content/major-investigation-and-public-protection/domestic-abuse/

This includes the current ACPO definition:

The cross-government definition of domestic violence and abuse is:

… any incident or pattern of incidents of controlling, coercive, 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. The abuse can encompass, but is not limited to:

- 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.

It is recognised that in order to meet the full range of social, welfare, economic, safety, accommodation, criminal and civil justice needs that individuals living with or escaping domestic abuse have, a multi-agency partnership approach is required.

To deliver the best safeguarding decisions that ensure timely, necessary and proportionate interventions, decision makers need the full information picture concerning an individual and their circumstances. Information viewed alone or in silos may not give the full picture or identify the true risk. All the information from various agencies needs to be available and accessible; to keep children and vulnerable adults safe and assist parties to this agreement in discharging their obligations under legislation.

2.1. DA MARAC

MARAC as a term is used to describe the Conference meetings themselves, and the work outside of the meetings. Sharing information through the MARAC enables agencies to act from a better factual understanding of the situation and of the risks faced by the victims. At the MARAC, agencies will discuss the likely outcomes of the proposed action plan to ensure that their combined actions are likely to promote the safety of, and reduce the risk to, the victims.

The purpose of a MARAC meeting is to:

- Share information to increase the safety, health and well-being of adult and child victims of domestic abuse.
- Jointly construct and implement a risk management plan that provides professional support to all those at risk, ensuring that agreed courses of action are carried out quickly and effectively.
- Identify underlying causes and any significant risk or safeguarding issues relating to the victim and/or perpetrators.
- Review cases and ensure that all possible strategies are considered for increasing the safety of victims and imposing sanctions to deter repeat offending.
- Reduce the risk of harm and increase the safety, health and wellbeing of victims and witnesses, both adults and children.
- Deliver a victim focussed approach - assessing the level of risk to the victim and putting measures in place to increase their safety and reduce the risk.
- Determine whether the perpetrators pose a risk to individuals or the general community.
- Address the perpetrator's behaviour using a balanced approach which considers prevention, interventions and enforcement.
- Reduce repeat victimisation.
- Support the government's Ending Violence Against Women and Girls Strategy 2016-2020 to develop safe and consistent policy and practice that supports the needs of all members of our diverse communities.
- Agree how the community and/or victim will be kept updated.

The coverage of a particular MARAC usually follows local authority borough boundaries. Regular and scheduled MARACs take place, with the inclusion of emergency conferences if, with the agreement of the MARAC Chair, a professional has serious concern for a case which requires immediate intervention.

2.2. DA MARAC Referrals

Safe Lives is a national charity dedicated to ending domestic abuse. Previously known as the Co-ordinated Action Against Domestic Abuse (CAADA), the charity worked with Association of Chief Police Officers (ACPO), now known as National Police Chiefs Council (NPCC), to create the Domestic Abuse, Stalking and Honour Based Violence (DASH) Risk Identification Checklist (RIC).

The DASH is a tool used to assess the immediate risk, threat and danger to which a survivor is subject. It is designed to be used for those suffering current rather than historic domestic abuse, and ideally would be used close in time to the last incident of abuse. The DASH should be used whenever a practitioner receives an initial disclosure of domestic abuse. Risk in domestic abuse situations is dynamic and can change very quickly, so a review of the checklist with a client may happen on more than one occasion.

Any professional should refer a case to the MARAC using the following thresholds, which are assessed using the DASH RIC:

- **Visible High Risk**
- **Escalation**
- **Professional judgement**

One or all these factors may apply for referring a case to the MARAC.

A MARAC to MARAC referral will be made when a victim moves between areas, either on a temporary (eg into refuge) or permanent basis. This is to ensure that there is continuity of support to victims.

2.3. DA MARAC Training

DA MARAC work is specialised and requires that staff taking part understand the context of the work, how domestic abuse can present, and the importance of safe and lawful information sharing. Each MARAC will establish what training is suitable to provide to participants and all parties agree to work collaboratively to ensure suitable training is provided and refreshed regularly.

Training should include:

- Understanding risk in the context of domestic abuse.
- Understanding how domestic abuse can present and how abuse may affect the ability and willingness of a victim to recognise or report abusive behaviour.
- The role of the MARAC in reducing risk to victims of domestic abuse.
- The MARAC process.
- Working in partnership – agencies' roles and responsibilities.
- Case studies – routes to and through the MARAC.
- Managing information legally and safely – why, when and how to share information.

All parties will also train and guide relevant teams to be aware of the work of MARAC and to actively consider making referrals in domestic abuse cases that present high risks to adults or children.

Additional guidance for a variety of practitioners is available on the Safe Lives website.

2.4. Independent Domestic Violence Advocates (IDVAs)

Independent Domestic Violence Advocates (IDVAs) are specialists who are Safe Lives accredited. They are trained to work with victims of domestic abuse at high-risk of serious harm. IDVAs provide high-risk victims of domestic abuse with a tailored and person-centred safety and support plan so that victims and their families are protected from abusive behaviour. This includes, but is not limited to, immediate risk assessment, safety planning, advocacy, emotional support and empowerment. The support lasts, on average, 2-3 months and enables clients to progress towards long-term safety. An IDVA's work can include court support, support within health services, housing advice, signposting and mediating between clients and services, and is always rooted in the safety of the victim and their family.

An IDVA can make a referral to MARAC on behalf of their client, and have referrals made to them by a MARAC.

2.5. Domestic Homicide Reviews (DHR)

The work of a MARAC supports the prevention of domestic homicides through timely, co-ordinated, and targeted intervention. Data discussed at a MARAC or MARAC outcomes may feature in a Domestic Homicide Review.

The Domestic Abuse, Crime and Victims Act 2004 places a duty on listed public bodies to undertake a "*review of the circumstances in which the death of a person aged 16 or over has, or appears to have, resulted from violence, abuse or neglect by—*

(a)a person to whom he was related or with whom he was or had been in an intimate personal relationship, or

(b)a member of the same household as himself, held with a view to identifying the lessons to be learnt from the death."

Those bodies are:

- chief officers of police for police areas in England and Wales
- local authorities
- local probation boards established under section 4 of the Criminal Justice and Court Services Act 2000 (c. 43)
- the National Health Service Commissioning Board
- clinical commissioning groups established under section 14D of the National Health Service Act 2006
- providers of probation services
- Local Health Boards established under section 11 of the National Health Service (Wales) Act 2006
- NHS trusts established under section 25 of the National Health Service Act 2006 or section 18 of the National Health Service (Wales) Act 2006

This legislation is underpinned by the Home Office *Multi-Agency Statutory Guidance for the Conduct of Domestic Homicide Reviews December 2016*.

The key purpose for undertaking a Domestic Homicide Review (DHR) is to enable lessons to be learnt where there may be links with domestic abuse. In order for these lessons to be learnt as widely and thoroughly as possible, professionals need to be able to understand fully what happened in each death, and most importantly, what needs to change in order to reduce the risk of such tragedies happening in the future.

2.6. Domestic Violence Disclosure Scheme (DVDS)

DVDS is a scheme with a very narrow focus – allowing police to disclose confidential data to reduce the threat of domestic violence posed by B to A. The scope of the risk assessment is broad, allowing for all data to be assessed and categorised. The scope of the disclosure is narrower but can include non-DA data if it is indicative of risk.

The police should consider DVDS when engaging on MARAC cases. If the suspect is known for violence, then the police officer handling the case will pass it to the DVDS SPOC to compile the wording before passing it to a Detective Inspector (DI) for authorisation. If approved, the disclosure takes place and MARAC are informed at the next meeting. This is to ensure that there is no further information to disclose and to put a safeguarding plan in place if necessary. By proactively reviewing all MARAC cases in this manner more potential DVDS disclosures are identified and are disclosed earlier.

This process means that there is a clear and identifiable process around ensuring that the highest risk cases and repeat victims are considered for DVDS. The process relies upon research that is already being conducted and therefore removes duplication of research and joins up the two processes.

2.7. Wanted Offenders

Whilst MARAC is a victim focused process, the sharing of information around wanted individuals perpetrating domestic abuse is an essential part of victim safeguarding. By sharing information held around wanted DA offenders with the police and other statutory bodies, victim risk can be successfully reduced.

The police can use the MARAC framework to request information from partners on a wanted offender and their whereabouts to effect lawful arrests. Successful apprehension and detention will reduce risk for victims and will reduce the volume of DA MARAC cases.

This information sharing can take place in writing, at a MARAC panel or across a virtual space if secure. Requests will be made as necessary. Each party has an obligation to assess what personal data is necessary and not excessive to share for the requester's stated purpose. Requests should be dealt with swiftly.

2.8. Wider safeguarding work

This agreement covers the sharing of information by the parties to the agreement. However, it is recognised that information is often provided to one or more of the agencies through referrals from individuals or organisations not subject to this DSA, such as a member of the public, a school or health practitioner. This is the nature of the welfare and safeguarding work being undertaken. Referrals may come originally through a MASH (Multi-Agency Safeguarding Hub) process and it is recognised that most of the parties to multi-agency safeguarding work are the same parties in this agreement.

2.9. Benefits

The benefits of this DSA are to:

- Cover the sharing of information for safeguarding and welfare purposes.
- Remove barriers to effective information sharing.
- Sets parameters for sharing personal data and clearly identifies the responsibilities of organisations.
- Identify the correct lawful basis to share personal information.

- Ensure information is shared whenever there is a requirement to do so.
- Enables authorities to share data on performance, quality assurance, learning and impact analysis.
- Raises awareness amongst all agencies of the key issues relating to information sharing and gives confidence in the process of sharing information with others.
- Support practitioners to understand what data can and should be shared.

The work of the DA MARAC is designed to support victims and perpetrators, reduce the risk of harm to individuals and improve outcomes. It brings together professionals from a range of agencies into a multi-agency forum to deliver a host of benefits.

Partner Agencies and Society

- Support increased mutual understanding of domestic abuse issues and the use of risk assessment techniques as well as increasing partners' knowledge of the success of different types of intervention strategies.
- Faster, more coordinated and consistent response to safeguarding concerns.
- A more accurate assessment of the risk and need, and the ability to modify plans in the light of information shared.
- A more thorough and focused management of all cases.
- Improving outcomes for victims.
- Better understanding between professionals.
- Avoiding the duplication of effort in respect of service provision and record taking and creating greater efficiencies in processes and use of resources.
- Preventing and detecting crime that impacts individuals and society.
- Delivering a safe environment overall for the public.

Individuals

- Timely action taken to reduce the risk of harm and increase the safety, health and wellbeing of victims and witnesses.
- A victim focused approach designed to support individuals and deliver comprehensive risk identification and safety planning based on a full account of the facts and circumstances of each victim's situation.
- The right sort and combination of advice, support and advocacy to be offered at the right time, based on a full and accurate account of the victim's needs and history, including other service contact and use.
- Victims to avoid the added distress of having to repeat details of their history or experience of domestic abuse and other circumstances each time they encounter a different service.
- Access to a Domestic Abuse Advocacy Service or another identified agency to act as the advocate for the victim at the MARAC and provide for two-way communication between the MARAC and the victim.

- Helping people who have been abusive towards their partners or ex-partners to change their behaviour and develop respectful, non-abusive relationships.
- Reducing risk of re-offending

2.10. Principles of information sharing

Effective information sharing is a vital element of both early intervention and safeguarding of vulnerable people at risk of harm or neglect. Organisations can hold different pieces of information which need to be placed together to enable a thorough assessment and plan to be made.

To share information, a lawful basis for doing so must be identified. This may come from legislation or from statutory guidance such as Working Together to Safeguard Children or the Children Act 2004, which places responsibilities on organisations outside of the parties to this DSA, such as sports clubs, private organisations, and the voluntary, community and faith sectors.

The sharing of personal data must comply with both the UK GDPR Principles and the Caldicott Principles, listed at Appendix A. Together, those principles lead to a series of questions and considerations to be answered before sharing takes place. These are listed as an Information Sharing Checklist in *Appendix D.*

2.11. Lawful Basis

The sharing of information must comply with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements. This is a complex area and each party must take their own decisions and seek advice from their organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian.

For purposes other than law enforcement by competent authorities

Articles 6, 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below.

Article 6 (1) – Personal Data Processing
(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject
(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller Use of this article requires that the Data Protection Act section 8 be satisfied. The laws given at *Appendix B – Applicable legislation* provide for each party a legal basis under section 8 – the specifics are noted in the appendix.
(f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party

Legitimate Interest will be the lawful basis for processing of personal data for the MARAC process for the third sector partner organisations, where they cannot rely on domestic abuse legislation and the Crime and Disorder Act and aren't classed as Competent Authorities. Consideration is given by each partner organisation to the three part test:

- The purpose test
- The necessity test
- The balancing test

Article 9 (2) – Special Category Personal Data Processing
(b) **social protection law** - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the **vital interests** of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(g) **substantial public interest** - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject Use of this article requires that the Data Protection Act Section 10(3) be satisfied. This requires that a condition within Schedule 1, Part 2 is met. For this agreement these are: ● *Statutory etc., and government purposes under Para 6(1)(2)* ● *Preventing and detecting unlawful acts under Para 10(1)(2)(3)* ● *Safeguarding children and individuals at risk under Para 18(1)(2)(3)(4)*
(h) **provision of health or social care** - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services Use of this article requires that the Data Protection Act Section 10(2) be satisfied. This requires that a condition within Schedule 1, Part 1 is met. For this agreement these are: ● *Health or Social Care Purposes under Para 2 with appropriate safeguards as required by section 11(1) of the act and Article 9(3) of the UK GDPR*

For the purposes of law enforcement by competent authorities

The 'competent authorities' are defined in Section 30 of the DPA which refers to Schedule 7. The competent authorities under this agreement are generally (but not exclusively) police, probation services, youth offending teams, government departments, and, in some cases, local authorities.

The law enforcement purposes are defined in Section 31 of the DPA as "*prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".*

There are additional safeguards required for sensitive processing. This is defined in Section 35(8) as:

(a) the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) the processing of genetic data, or of biometric data, for the purpose of uniquely identifying an individual;

(c) the processing of data concerning health;

(d) the processing of data concerning an individual's sex life or sexual orientation.

The additional requirements are given in Section 35(4) and (5). Both require an appropriate policy document, and this document will form part of the policy for such processing, although competent authorities will need to satisfy themselves their own internal policy documents fully cover such use.

Compliance is through section 35(4), which requires the consent of the data subject, or through section 35(5), which requires that the processing be strictly necessary for the law enforcement purposes, and meets a condition in Schedule 8. Consent is unlikely to be appropriate for this work.

For the processing in relation to the purposes here, the following conditions in Schedule 8 are met:

- Statutory etc. purposes Para 1(a)(b);
- Administration of justice Para 2;
- Protecting individual's vital interests Para 3;
- Safeguarding of children and of individuals at risk Para 4(1)(2)(3)(4);

The applicable legislation that provides the lawful basis is listed in more detail in *Appendix B – Applicable legislation.*

2.12. Consent

The parties will often work collaboratively with victims and witnesses, and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) or explicit consent (Article 9 (a)) as the lawful basis conditions used for processing under this agreement.

Consent is not generally the lawful basis that public sector organisations use for processing information shared under this agreement. It is possible that the other parties, such as voluntary groups, may use consent as lawful basis for some personal data processing. Each party is responsible for managing consent where they use consent as a lawful basis condition.

2.13. Proportionality and necessity

Proportionality and necessity are factors to be taken into consideration when deciding whether to share personal information. In making the decision, employees must weigh up what might happen as a result of the information being shared against what might happen if it is not, and apply their professional judgement.

Although sharing of information can impact on a practitioner's relationship with an individual/family, avoiding serious harm to an individual must be the first consideration. Safeguarding is a 'special purpose' under the Data Protection Act and as such you should share if the sharing is necessary for protection an individual or a type of individual who is under 18 or over 18 and at risk from neglect or physical, mental or emotional harm.

You are expected to justify that you believed sharing was necessary for one of the following criteria:

- necessary for the purposes of preventing or detecting crime
- required or authorised by an enactment, by a rule of law or by the order of a court or tribunal
- in the particular circumstances, was justified as being in the public interest.

Or that you acted in the reasonable belief that:

- the person had a legal right to do the obtaining, disclosing, procuring or retaining, or
- the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it

Only the personal data necessary for the stated purpose or request at hand should be shared. Sharing must not be excessive. This may mean sharing less personal data than has been requested.

2.14. Other relevant legislation

The actual disclosure of any personal data to achieve these objectives must be conducted within the framework of the Human Rights Act 1998 (HRA) and the Common Law Duty of Confidence. Caldicott Principles also apply to all information sharing and they are listed in Appendix A.

- Human Rights Act 1998 (HRA)
- Common law duty of confidentiality
- Confidentiality and Sharing for Direct Care

2.15. Common Law Duty of Confidence

Much of the police information to be shared will not have been obtained under a duty of confidence as it is legitimately assumed that data subjects will understand that police will act appropriately with regards to the information for the purposes of preventing harm and domestic abuse.

Information held by other agencies that will be shared in the MARAC process may have been gathered where a duty of confidence is owed. Duty of confidence is not an absolute bar to disclosure as information can be shared where there is a strong enough public interest to do so.

When overriding the duty of confidentiality, the parties may seek the views of the organisation who hold the duty of confidentiality and consider their views in relation to breaching confidentiality. The organisation may wish to seek legal advice if time permits.

2.16. Freedom of Information

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply, and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations' FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who holds the information (data controller).

It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place. A Data Protection Impact Assessment (DPIA) is the designated tool.

Even where a DPIA is not mandatory under data protection legislation, the ICO's statutory guidance in the Data Sharing Code of Practice recommends a DPIA where the personal data of vulnerable individuals and children is being processed and shared. Each party agrees that they have undertaken a DPIA, where they feel the processing meets the legislative criteria for a DPIA.

3.1. Right to be informed – Privacy notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of data protection legislation and will issue appropriate notices which inform the data subject that the information will be shared with the parties under this agreement.

In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. The nature of the data and data subjects means that the exemptions to the data subject rights described in the DPA 2018 Part 2, Chapter 2, s15, and in Schedule 2, Part 1, para 2 (crime and taxation) and Schedule 3, Part 3, para 11 (serious harm) will often apply to the processing and sharing of data under this agreement.

Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals

that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware.

3.2. Data subject rights requests and complaints

Each organisation must have in place appropriate policies and processes to handle data subject requests made under data protection law, to ensure they are responded to within deadline and in an appropriate manner. Requests include right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision-making including profiling. As described in 3.1 above, the exemptions available in the DPA 2018 allow the signatory parties to withhold information requested under a data subject's rights.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties where relevant and appropriate. Each party is then responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair and objective complaint procedures. Any complaints from individuals how their data is being processed or shared will be handled under the policy and processes of organisation concerned.

3.3. Data subjects

There is a breadth of data subjects whose data is shared under this agreement. The data subjects include the following:

- victims
- family members, carers and other persons whose presence and/or relationship is relevant to identifying and assessing the risks to individuals
- actual or suspected perpetrators
- professional adviser or consultant (eg doctor, lawyer)
- professional opinions of employees eg social workers and police officers
- witnesses

Many of the data subjects are vulnerable. Parties to this agreement are in positions of power over data subjects and data subjects have little or no control over why and how their data is processed.

4. Data

The personal data and its processing involved in these workstreams is extensive, highly sensitive and at times intrusive. There is a high volume of data and data subjects. Anonymisation or pseudonymisation will rarely be possible because of the way the work focuses on individuals, although any statutory returns, workforce planning and management reports should be anonymised if possible.

Information will include:

- **Personal, special category and criminal data** to enable the swift and effective safeguarding of children and improved safeguarding provision in the borough
- **Personal, special category and criminal data** for law enforcement purposes, including data defined as **sensitive data** for the competent authorities for law enforcement purposes
- **Aggregated (anonymised or pseudonymised) data** reporting to enable the partnership to further understand the safeguarding priorities.
- **Aggregated (anonymised or pseudonymised) and personal data** regarding employees in relation to serious case reviews, investigations into allegations against staff, learning review and workforce development.
- **Personal and anonymised data** required for statutory returns.

4.1. The data to be shared

Due to the complexity of the domestic abuse and MARAC processes, providing a prescriptive list of data fields to be shared is difficult. Not all the personal data will be shared in every case; only relevant information will be shared on a case-by-case basis where an organisation has a need to know the information.

Data that will be shared includes:

- Name, address and contact details
- age/date of birth
- ethnic origin, religion and other equalities information
- physical description
- family composition and relationship information, including information on people who are significant in a victim's life and whose influence is potentially detrimental to their safety and/or wellbeing; with details of the reasons for these concerns
- criminal information on allegations and convictions, police intelligence, anti-social behaviour (ASB) data
- school and educational information
- health records including NHS number, involvement with GP, London Ambulance Service and other
- information about injuries including Female Genital Mutilation (FGM) and evidence of abuse
- information on gender, sex life and sexual orientation
- housing information
- social services information, referrals and assessments
- financial information
- images in photographs, film or CCTV
- employment information

Police information will be:

Custody images

Convictions / offending history

Crime reports – details of offence

Merlin reports – the report in its entirety is shared with YOS

Custody record – where necessary

Criminal Intelligence reports – redacted where appropriate

Details of incidents that indicate risk and vulnerability

4.2. Deceased persons

It is noted that the sharing will involve data of deceased persons. This data will not be covered by data protection legislation but will still require due regard to the common law duty of confidentiality and the Human Rights Act.

4.3. Confidential information

In this agreement, we refer to personal data, as defined by data protection legislation. However, the word 'confidential' may be used by individuals and practitioners to describe information and can mean different things to different people.

Confidential can mean:

- Personal and special category data as defined by data protection legislation
- Patient Identifiable Information (PII) or 'personal confidential information'; both terms most commonly used in health settings
- Information which is not already lawfully in the public domain or readily available from another public source
- Information that has been provided in circumstances where the person giving the information could reasonably expect that it would not be shared with others.

4.4. Storing and handling information securely

Information should only be stored and shared in accordance with data protection legislation and follow information security policies and procedures of the relevant organisation. Information should always be shared securely, either by a secure IT connection, encrypted email, or secure and tracked transfer of paper documents. Information should never be sent via a non-secure method. The employee/organisation sending the information must choose the most appropriate method of transfer and be responsible for its safe delivery.

Email is not generally a secure method of transferring personal data. Although two or more of the parties may have encryption that allows for an encrypted path between them, it would be prudent for parties to establish whether there are any encrypted paths between them, and write that into the organisation's processes for employees.

In the absence of such pre-established secure pathways, secure email systems such as CJSM, Egress and Encrypt and Send can be used, or systems that allow for secure file sharing. Description of specific transfer processes must be in relevant process documents within each organisation.

Information may be shared over the phone, in a virtual meeting, or a face-to-face meeting. Employees must ensure that attendance and distribution of content is limited to only what is necessary, with distribution of minutes or recordings limited to only those necessary.

Sharing by telephone should be avoided unless the requirement is urgent, and email is not practicable. You must ensure you are in a place where you cannot be overheard, including by smart tech or 'Internet of Things' devices, like Alexa, Siri etc.

Any paper records printed must be kept to a minimum and kept secure at all times whether in the office, home or during transit. Organisations must adopt an appropriate policy surrounding the use and transfer of paper records. Appropriate security methods must be applied when storing or disposing of paper records.

4.5. Access controls and security

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted. Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources of the relevant employer.

4.6. Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that suitable written agreements are in place, and that appropriate due diligence has been completed for the transfer of data.

4.7. Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality.

Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.

4.8. Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This must include assessing the level of risk to the data subject(s), as well as to make a decision on notifying the ICO within the statutory time frame of 72 hours.

This complies with Articles 33 and 34 of UK GDPR, and Section 67 and 68 of the DPA 2018 for personal data processed for law enforcement purposes.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed as quickly as possible given the risk to individuals, and appropriate co-ordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

All parties agree that security breaches (including misuse or unauthorised disclosure) are covered by their internal disciplinary procedures. If misuse is found there is a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.9. Retention & Disposal

Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.

Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.

5. Signatures

For the Metropolitan Police:

Agreed as appropriate for business use by;

Metropolitan Police Service

Date:

Probation Service and Local Authorities: will sign this DSA via a centralised electronic system rather than physically signing a document.

Version control	
Document production date	August 2021 Finalised Jan 2022
Document currency	Final 1.0

6. Appendices

6.1. Appendix A: Parties to this agreement

Organisation	Duties
Metropolitan Police	• The prevention and detection of crime • The maintenance of the Queen's peace • Protection of the vulnerable
London Borough	• Co-ordinates, gathers, processes, risk assesses and shares information held about all the areas covered in the DSA in conjunction with information received from partner agencies, to enable the council to undertake its statutory duties in these areas • Makes decisions on whether to undertake enforcement or other appropriate actions under its powers in the legislation listed in this DSA • Allocates resources in accordance with priority of tasks and policies • Co-ordinates, gathers, processes, risk assesses and shares information covering all the areas under this DSA with partners to achieve common goals • Undertakes interventions as necessary to ensure the safeguarding of vulnerable people • Decides whether to undertake prosecutions when offences covered by the legislation in this DSA has been breached and it is within the council's remit • Takes appropriate and proportionate steps to ensure the safety of employees and others
Probation Service	• The Probation Service is a statutory criminal justice service that supervises high-risk offenders released into the community. • Provide risk assessment and sentence planning • support of offenders in coming to terms with their sentence, the root causes of the crime and providing advice

7. Appendix A : Data Protection & Caldicott Principles

The Principles as described in Article 5 of the General Data Protection Regulation.

1) Fair & Lawful
processed lawfully, fairly and in a transparent manner in relation to the data subject

2) Purpose limitation
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

3) Data minimisation
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4) Accuracy
accurate and, where necessary, kept up to date; Inaccurate data must be erased or rectified without delay

5) Storage limitation
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

6) Integrity & Confidentiality
secured through appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

7) Accountability
processed by organisations that take responsibility for the personal data, with appropriate measures and records in place to demonstrate compliance.

The Caldicott Principles

Principle 1
Justify the purpose(s) for using confidential information
Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2
Use confidential information only when it is necessary
Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3
Use the minimum necessary confidential information
Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4
Access to confidential information should be on a strict need -to-know basis
Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5
Everyone with access to confidential information should be aware of their responsibilities
Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6
Comply with the law
Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7
The duty to share information for individual care is as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8
Inform patients and service users about how their confidential information is used
A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. As a minimum, this should include providing accessible, relevant and appropriate information. In some cases, greater engagement will be required.

8. Appendix B – Applicable legislation

Legislation	Main purpose of Legislation
Domestic Abuse, Crime and Victims Act 2004	Legislates for the apprehension and prosecution of offenders, investigatory instructions and support for victims and witnesses. Also places a duty on public bodies listed in the legislation to undertake Domestic Homicide Reviews.
The Crime and Disorder Act 1998[1]	Each LA in England & Wales has the responsibility to formulate a strategy to reduce crime and disorder in their area and to work with police authorities to do this.
Multi-Agency Statutory Guidance for the Conduct of Domestic Homicide Reviews December 2016	Statutory guidance under section 9(3) of the Domestic Violence, Crime and Victims Act 2004 (the 2004 Act) covering the delivery of Domestic Homicide Reviews.
Controlling or Coercive Behaviour in an Intimate or Family Relationship Statutory Guidance Framework December 2015	Guidance mainly for police and criminal justice agencies, on identifying domestic violence, domestic abuse and controlling or coercive behaviour; circumstances in which the new offence might apply; the types of evidence for the offence; the defence.
The Police and Criminal Evidence Act 1984	This act makes the specific provision for the secretary of state to issue codes of practice to police with statutory effects. It provides the basis for many of the police actions in respect of matters relating to safeguarding and other matters, and as such provides their legal basis for use.
The Education Act 2002[2]	The Education Act 2002 puts a duty on schools to exercise their functions with a view to safeguarding and promoting the welfare of children. All schools are required by law to teach a broad and balanced curriculum which promotes the spiritual, moral and cultural development of pupils and prepares them for the opportunities, responsibilities and experiences of life. This regulation provides specific powers for dealing with school-related safeguarding and welfare issues giving a legal basis under Section 8 of the DPA for this use.
The Children Act 1989	Under S.47 of the *Children's Act 1989*, a Local Authority has a duty to investigate when informed that a child in their area is in police protection or the subject of a protection order. This regulation provides specific powers giving a legal basis under Section 8 of the DPA for this use.
The Children Act 2004	Under Sections 10 and 11 of the *Children Act 2004*, the police, local authorities and primary care trusts must co-operate with other relevant partners to

[1] http://www.legislation.gov.uk/ukpga/1998/37/contents
[2] http://www.legislation.gov.uk/ukpga/2002/32/contents

	safeguard and promote the welfare of children and ensure that arrangements are made to improve the wellbeing of children in their area. This regulation provides a general safeguarding and welfare power giving a legal basis under Section 8 of the DPA for this use
The Children & Social Work Act 2017[3]	The Children and Social Work Act 2017 (the Act) is intended to improve support for looked after children and care leavers, promote the welfare and safeguarding of children, and make provisions about the regulation of social workers. The Act sets out corporate parenting principles for the council as a whole to be the best parent it can be to children in its care. These are largely a collation of existing duties local authorities have towards looked after children and those leaving care.
The Health and Social Care Act 2012[4]	This act provides for the delivery of Health and Social Care, providing a legal basis for many of the services delivered by parties to this agreement. In particular, it places (section 251B) a duty to share information relating to health and adult social care unless the data subject has specifically objected. This regulation provides a specific duty giving a legal basis under Section 8 of the DPA for this use.
FGM Mandatory Guidance[5]	Section 5B of the 2003 Act introduces a mandatory reporting duty which requires regulated health and social care professionals and teachers in England and Wales to report 'known' cases of FGM in under 18s which they identify in the course of their professional work to the police. The duty applies to all regulated professionals (as defined in section 5B(2)(a), (11) and (12) of the 2003 Act) working within health or social care, and teachers. The legislation requires regulated health and social care professionals and teachers in England and Wales to make a report to the police where, in the course of their professional duties, they either: ● are informed by a girl under 18 that an act of FGM has been carried out on her; or, ● observe physical signs which appear to show that an act of FGM has been carried out on a girl under 18 and they have no reason to believe that the act was necessary for the girl's physical or mental health or for purposes connected with labour or birth.
Department for Education Information Sharing for Practitioners 2018[6]	This HM Government advice is non-statutory, and has been produced to support practitioners in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being. The advice is for all frontline practitioners and senior managers working with children, young people, parents and carers who have to make decisions about sharing personal information on a case-by-case basis.

[3] http://www.legislation.gov.uk/ukpga/2017/16/contents
[4] https://www.legislation.gov.uk/ukpga/2012/7/contents
[5] https://www.gov.uk/government/publications/mandatory-reporting-of-female-genital-mutilation-procedural-information
[6] https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

The Local Government Act 2000[7]	The main principles of the Local Government Act 2000 are to give powers to local authorities to promote economic, social and environmental well-being within their boundaries. This was mostly replaced by the Localism Act 2011 below, but still applies in Wales.
London Child Protection Procedures 2018[8]	Procedures which all London agencies, groups and individuals must follow in identifying, raising and responding to welfare concerns when coming into contact with or receiving information about children 0 to 17 years, including unborn children and adolescents up to their 18th birthday This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for various London bodies.
Working Together to Safeguard Children	Local authorities, working with partner organisations and agencies, have specific duties to safeguard and promote the welfare of all children in their area. The Children Acts of 1989 and 2004 set out specific duties: section 17 of the Children Act 1989 puts a duty on the local authority to provide services to children in need in their area, regardless of where they are found; section 47 of the same Act requires local authorities to undertake enquiries if they believe a child has suffered or is likely to suffer significant harm. This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for national bodies.
Human Rights Act 1998	Article 2.1 stipulates that “Everyone’s right to life shall be protected by law”. Article 3 stipulates that “No one shall be subjected to torture or to inhuman or degrading treatment or punishment”. Article 6 stipulates the right to a fair trial. Article 8 stipulates that “Everyone shall have the right to respect for his private and family life, his home and correspondence….. There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. Articles 2.1 and 3 may create a duty on public sector bodies to share information in order to protect individuals from serious threats to their physical safety or wellbeing. On the other hand, article 8 may prohibit public sector bodies from sharing personal information in cases where such sharing cannot be justified as being necessary for

[7] http://www.legislation.gov.uk/ukpga/2000/22/contents
[8] http://www.londoncp.co.uk/

	one of the objectives listed in article 8.2.
NHSE Safeguarding Vulnerable People in the NHS – Accountability and Assurance Framework 2015 [9]	It sets out safeguarding roles, duties and responsibilities of all organisations commissioning NHS health and social care. The framework aims to: ● Identify and clarify how relationships between health and other systems work at both strategic and operational levels to safeguard children, young people and adults at risk of abuse or neglect. ● Clearly set out the legal framework for safeguarding as it relates to the various NHS organisations in order to support them in discharging their statutory requirements to safeguard children and adults. ● Promote empowerment and autonomy for adults, including those who lack capacity for a particular decision as embodied in the Mental Capacity Act 2005 implementing an approach which appropriately balances this with safeguarding. ● Outline principles, attitudes, expectations and ways of working that recognise that safeguarding is everybody's business and that the safety and well-being of those in vulnerable circumstances is at the forefront of our business. ● Set out how the health system operates, how it will be held to account both locally and nationally and make clear the arrangements and processes to be undertaken to provide assurance to the NHS England Board with regard to the effectiveness of safeguarding arrangements across the system; and ● Outline how professional leadership and expertise will be developed and retained in the NHS, including the key role of Designated and Named Professionals for Safeguarding Children and Designated Adult Safeguarding Managers This provides the policy document required for the safeguarding purposes under Schedule 1 Part 2, para 18 of the DPA for the NHS bodies,

●

[9] https://www.england.nhs.uk/wp-content/uploads/2015/07/safeguarding-accountability-assurance-framework.pdf

9. Appendix C: Information Sharing Checklist

The following questions must be considered when deciding whether to share information.

- Whose information is this?
- Is there a lawful basis to share the information? Justify the purpose and identify relevant legislation that applies.
- Can information be pseudonymised or anonymised ahead of sharing?
- How have individuals been informed that the information will be shared eg via a privacy notice? Will they have the expectation that their information will be shared? Consider whether notifying the individual of the sharing may place someone at risk or prejudice a police or safeguarding investigation.
- Have any requests not to share been received and considered?
- How much information is it necessary to share in this situation?
- Is the information accurate and up to date? Has the difference between fact and opinion been stated?
- Is access to the information limited to only those who need it? Is it being given to the right person?
- Is the information being shared in a secure way?
- Has the decision to share or not share been recorded?

10. Appendix D: Conference Protocol

Frequency

Each DA MARAC will decide on the necessary frequency of conferences, to discuss high-risk cases and share information about the parties involved to allow action to be taken to manage the risk posed to the victim/victim and any children. This includes emergency MARACs.

Information sharing

The information will be shared between designated and named representatives from the signatory parties, and with other agencies identified as relevant by the local DA MARAC Co-ordinator on a case-by-case basis. These agencies include community based and voluntary perpetrator programmes, local drug and alcohol services, child and family support organisations.

Confidentiality

Confidentiality of the MARAC is paramount. At the start of each MARAC the Chair will read out the confidentially agreement, which all attendees are expected to follow; that information discussed within the meeting is sensitive and must not be disclosed to a third party without the agreement of the parties at the meeting.

Any virtual attendees have responsibility for confidentiality of the meeting, such as ensuring they are in a location where they cannot be overheard, and their screen cannot be seen. The MARAC Chair should remind attendees of this responsibility before the meeting begins.

MARAC process

Each domestic crime/incident recorded by the police is subjected to a risk assessment, firstly utilising the DASH model and, in high-risk cases, completion of a Part 2 Risk Assessment. A sergeant will supervise all risk assessments. Those identified, as being at high risk will be referred to the police DA MARAC co-ordinator for further referral to the IDVA Service and DA MARAC. The details of the victim, their children and the perpetrator will then be forwarded to the DA MARAC group attendees within locally agreed timescales, prior to the meeting, to enable them to collate the information that they hold on the nominated parties that may assist in safety planning and risk management.

Other members of the DA MARAC have the facility to refer high risk victims to the MARAC by use of the local bespoke referral form (compiled individually by each MARAC) which is sent to the DA MARAC Co-ordinator within the same timescales.

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

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

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

The source of police information will be from a number of databases including: Police National Computer, CRIS, CRIMINT, Merlin, 124D (domestic abuse notebook), Part 2 Risk Assessments, Independent Domestic Abuse Advocacy Service referral forms, MARAC partner agency referral forms, and individual case files on high risk victims. The information provided will be sufficient for partner agencies to interrogate their indices to establish if the parties are known to them, thus enabling them to provide further information to all the MARAC group in order to provide a holistic view to the threat posed to the victim(s).

11. Appendix E: Conference Confidentiality Statement

This statement (or a locally agreed substitute) will be read out at the beginning of each conference. All attendees must comply, or identify to the Chair before the meeting begins if they are unable to comply and why. The Chair will take the decision of whether the attendees can continue within the meeting.

The Chair of the Meeting reminds all attendees of the requirements and protocols within the Multi-Agency Risk Assessment Conference (MARAC) Data Sharing Agreement.

The purpose of this conference is to share information/data for the purpose of making, modifying and implementing plans to support the reduction of future harm for very high-risk domestic abuse victims. The responsibility to take appropriate actions rests with the individual agencies; it is not transferred to the MARAC. This includes responsibilities for the sharing of information under this agreement.

All individuals who are discussed at the conference will be treated fairly, with respect and without discrimination. All work at conference will be informed by a commitment to equal opportunities and effective practice issues in relation to race, gender, sexuality and disability, and by the duty to protect the confidentiality of the personal data of the individuals discussed.

Information discussed within the conference is confidential and must not be disclosed to third parties unless they are a signatory to the DA MARAC Data Sharing Agreement, or when it has been agreed by the partners at the conference.

Hard copies of information brought to or received at the conference will be left in the meeting room, where the DA MARAC Co-ordinator is responsible for secure disposal. If attending virtually, you must ensure you are in a place where you cannot be overheard, including by smart tech or 'Internet of Things' devices, like Alexa, Siri etc. All agencies must ensure that the minutes are retained securely in line with the agency's retention schedule.

Date of Conference: _____

By signing the attendance sheet agency representatives agree to abide by this agreement.

Name	Job Title	Organisation