Multi Agency Risk Assessment Conference (MARAC)

Information Sharing Agreement

Document Management

Document Disclaimer

This document is issued only for the purpose for which it is supplied.

Document Owner
This document is produced and owned by Staffordshire Police. It is the responsibility of the thematic lead officer to review and update annually and as required.

Document Control
This document is controlled and maintained according to the documentation standards and procedures of Staffordshire Police. All requests for changes to this document must be sent to the Head of Domestic Abuse for sign off.

Distribution List
This document is published on the intranet for access by all users and will be sent to the recipients as defined within the distribution.

Change History

Version	Author (s)	Reason for Change	Date
0.1	Paul Rushton (Police)	Initial Agreement	22nd March 2011
0.2	Martine Redpath	Update	1st July 2014
0.3	John Maddox and Natalie Morrissey	Compliance with GDPR and DPA 2018 (Pre DPA 2018)	April 2018
0.4	John Maddox & Natalie Morrissey	Post GDPR & DPA Implementation	October 2018

Approvals

Version	Name	Position	Date Approved
0.4	DCI Simon Brownsword	Domestic Abuse Thematic lead	

This Individual Agreement is made under the One Staffordshire Information Sharing Protocol between:

Partners: Competent Authorities (not listed below) as per Schedule 7 of DPA 2018
Staffordshire Police
Staffordshire County Council

Stoke-on-Trent City Council
District and Borough Councils
NHS Provider Trusts
Housing Associations
Commissioned service providers
Schools and other educational establishments
Clinical Commissioning Groups
General Practitioners
National Probation Service
Community Rehabilitation Companies
Voluntary Sector Agencies

(This is a general list and agencies who are local or not covered above can nevertheless sign upto this agreement).

Context: A MARAC, [multi-agency risk assessment conference], is a meeting where information is shared on the highest risk domestic abuse cases between representatives of local Police, Probation services, Health, Children's Social Care, Housing providers, Independent Domestic Violence Advisors (IDVAs) and other specialists/professionals from the statutory and voluntary sectors or interested parties relevant to the case. In Staffordshire & Stoke on Trent MARAC is more than just a meeting it is part of a process of dealing with the risk that victims and wider family members experience from domestic abuse. It involves an end to end process to increase the safety of the victim and other vulnerable parties such as children. The MARAC then creates a multi-agency action plan to address the identified risks and increase the safety and wellbeing of all those at risks. UK law priorities the safety of children and MARAC activity will complement (not duplicate) provision of safety planning in such cases as well as taking action to address perpetrator behaviour.

1. **Legal Basis for sharing:**

1.1. The MARAC is a local, multi-agency meeting where information will be shared between agencies regarding high risk cases of domestic abuse.

1.2. The sharing will take place underpinned by a legal basis using the powers that each agency relies on to carry out their professional roles & responsibilities. Agencies will have in depth knowledge of this enabling legislation e.g. section 115 crime & disorder act 1998.

1.3. Personal data must only be processed where specific conditions of the Data Protection Act 2018 and the General Data Protection Regulations are met.

1.4 **General Data Protection Regulations** The GDPR sets out six key principles, accountability is accepted as an additional principle and should be considered in all processing.

- Lawfulness, fairness and transparency (accepting that Law Enforcement under DPA 2018 does not include transparency)
- Purpose limitation

- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- (Accountability)

1.5 Article 6 of GDPR sets the lawful basis for processing which include:

You must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. It is important to emphasise that ICO advice is that consent is difficult for public authorities to achieve because of the imbalance of power (see GDPR consent guidance).

- **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **(d) Vital interests:** the processing is necessary to protect someone's life.
- **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

1.5.1 For MARAC cases, the following are the legal basis primarily relied upon in such cases:

(c) Processing is necessary for **compliance with a legal obligation** (article 6 (c) 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. (Vital interest refers to matters of life or death)

(e) Processing is necessary for the performance of a task carried out in the **public interest** Article 6(e) or in the exercise of official authority vested in the controller.

(f) Those partners that are from the private sector can process personal data without consent if there is a genuine and legitimate reason which includes

commercial benefit unless this is outweighed by harm to the rights of the individual. **Legitimate Interest** (article 6(f).

1.5.2 For a list of legislative authorities see appendix B

1.6 Article 9 of GDPR: apply where the personal data is **sensitive/special category**. This data is more sensitive and so needs more protection. This includes information in relation to:
Race;
Ethnic origin;
Politics;
Religion;
Trade union membership;
Genetics;
Biometrics (where used for ID purposes);
Health;
Sex life; or
Sexual orientation

1.7 In order to share/process personal data falling in this category you must identify both a lawful basis under article 6 AND a separate condition under article 9. They do not however have to be linked. Article 9 (b, c & g) condition that MAY be relied upon in order to share information in this context however reference to the full article should be considered in every case…

B – Processing is necessary for the purpose of carrying out the obligations and exercising of 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 law or a collective agreement pursuant of the law for appropriate safeguards for the fundamental rights and the interests of the data subject.
C – 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 - For reasons of **substantial public interest** in accordance with the 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.

1.8 The Guide to Law Enforcement is separate to GDPR and is contained within Part 3 of the Data Protection Act 2018.

1.9 This part of the Act transposes the EU Data Protection Directive 2016/680 (Law Enforcement Directive) into domestic UK law. The Directive complements the General Data Protection Regulation (GDPR) and sets out the requirements for the processing of personal data for criminal 'law enforcement purposes'.

2.0 Law enforcement applies to, but not limited to, the police, criminal courts, prisons, non-policing law enforcement and any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

2.1 Law Enforcement purposes means; **the 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.

2.2 Any competent authority relying on part 3 of DPA 2018 will apply the six principles of DPA 2018 as summarised by chapter 2, the abbreviated summary directs agencies to the relevant sections of the act

- Processing be Lawful & fair - sec 35(1) (note GDPR adds transparency here, see above)
- Purpose for processing be specified, explicit and legitimate – sec36(1)
- Personal data be adequate, relevant and not excessive – sec 37
- Personal data be accurate and kept upto date – sec 38(1)
- Personal data be kept no longer than necessary – sec 39(1)
- Personal data be processed in a secure manner – sec 40

2.2.1 Special category data-processing for Law Enforcement purposes can be undertaken if the following conditions apply under schedule 8 (1-9) DPA 2018;

2.2.2 The processing is necessary for the exercise of compliance with **UK law** or it is necessary for reasons of **substantial public interest**.

2.2.3 Processing is necessary for the **administration of justice**

2.2.4 Processing is necessary to protect the **vital interests** of the data subject or another individual.

2.2.5 **safeguarding of children and of individuals at risk** (subsection 4(1) Processing is necessary for:

a) the purpose of protecting an individual from neglect or physical, mental or emotional harm, or
protecting the physical, mental or emotional well-being of an individual
b) the individual is aged 18 or under, or
aged 18 or over and at risk
c) the processing is carried out without the consent of the data subject

2.2.6 (9b) 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.

2.2.7 (9c) 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

2.2.8 (9g) processing is necessary for reasons of substantial public interest, on the basis of UK 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

2.2.9 (9h) 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 on the basis of UK law or pursuant to contract with a health professional.

2.3.1 Wherever possible the individual will **consent** to any data that will be shared however in some circumstances data may be shared without consent where it is lawful to do so. Consent is not always conducive or appropriate in law enforcement scenarios.

2.3.2 Furthermore the ICO advises that public authorities in a position of power over individuals should avoid relying on consent.

3.0 **Purpose for the sharing:**

3.1 The sharing is necessary to enable agencies to work together to protect and support victims and their families and reduce repeat offending. Domestic abuse is defined by the Home Office[1]

3.2 This agreement will also assist in:

3.2.1 Enabling partners to direct services accordingly and into areas most at need.

3.2.2 Identifying the true level of domestic abuse incidents throughout the County of Staffordshire and the City of Stoke on Trent.

3.2.3 Identifying and arranging adequate measures to protect children

3.2.4 Supporting funding opportunities.

3.2.5 Preventing crime and disorder in the Staffordshire & Stoke on Trent area.

3.2.6 Assisting in the prosecution of offenders.

3.2.7 Assisting the Performance Indicator targets and other strategic targets which include domestic abuse measures

3.2.8 Identifying training needs.

3.2.9 Identifying successes and failures of projects/services/initiatives.

3.2.10 Improving inter agency working.

3.2.11 Identifying root causes of domestic abuse

3.2.12 The administration and function of M.A.R.A.C.'s.

3.2.13 The administration and function of Domestic Abuse Homicide Reviews.

4 **Type of information that may be shared:**

4.1 There will be three types of data that may be shared under this agreement:

[1] https://www.gov.uk/guidance/domestic-violence-and-abuse

4.1.1. Personal data: Any information that will allow the individual to be identified.
4.1.2 Sensitive Personal Data: As listed within this agreement
4.1.3 De-personalised (or anonymised) data: Information which no longer allows the individual to be recognised.

4.2 Agencies may share data about any individual identified including victims, children, perpetrators.

5 General Roles and Responsibilities

5.1 It is vital that agencies who have a role in supporting the victim consistently attend the M.A.R.A.C. in order for the meeting to be effective. That said carrying out actions is equally important in relation to reducing risk and any such update should be available to the meeting process.

5.2 Multi-agency partners will be equal partners, and responsibilities are defined by their own organisation and the public interest and will be accountable to the M.A.R.A.C. meeting for ensuring that these agreed responsibilities are carried out.

5.3 Multi-agency partners will support the principles and purpose of the M.A.R.A.C. which is to promote the safeguarding of victims of domestic abuse, and their immediate family members, including any children involved.

5.4 The M.A.R.A.C. is held as required, as it is imperative that very high-risk cases are dealt with in a timely fashion that allows for earlier interventions.

5.5 Referrals will come from the Police and any other agency that completes the appropriate Risk Assessment Form. Referrals will be based on presenting circumstances and extent of abuse, or on professional judgement. Threshold decisions are taken in MASH (Multi-agency safeguarding Hub) where additional information will be overlaid to achieve a further risk evaluation.

5.6 Any information disclosed will have a legal basis identified as determined in this agreement (see paragraph 1) in order that a duty of care can be met by the partners to this agreement. It is good practice to ensure all involved are informed of the case and what activity is being undertaken in order to adhere to the principles of GDPR although this is not itself consent and it is not essential. What must be born in mind is that true consent empowers individuals, is freely given, specific, informed and unambiguous. Any consent should be granular and actively managed as an ongoing process. As a legal basis it allows individuals to make further choices in their rights such as to withdraw consent and enact the right to erasure of their data. *AKA right to be forgotten.*

5.7 During the M.A.R.A.C. the Chair will seek clarification from the agencies to verify whether the victim is aware that they are a subject of the M.A.R.A.C. as it is good practice that victims are aware of activities that are taking place to ensure their safety and that of their family. If it is clearly established that the victim is not aware, the Chair should ensure a victim service provides clarity on this issue, when it is safe to do so.

6 Confidentiality

6.1 It will be deemed necessary for agencies attending the M.A.R.A.C. to be made aware by the Chairperson of a strict confidentiality policy, which is to be adopted. All attendees will sign the confidentiality statement at **Appendix A**.

6.2 No agency should share information with a third party which has emanated from the M.A.R.A.C. meeting, unless an overriding public interest to do so or the disclosure is required by law. Any such activity must be subsequently reported to the MARAC case co-ordinator asap.

6.3 **Data Controller**

The GDPR applies to 'controllers' **and** 'processors'.
A controller determines the purposes and means of processing personal data.
A processor is responsible for processing personal data on behalf of a controller.

6.4 The controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

6.5 MARAC is made up of agencies who fulfil a role that meets that of controller and who implement appropriate technical and organisational means by design and default in order to comply with DPA 2018.

6.6 Notwithstanding that partners may be controllers in their own right the combining of data for the effective function of a MARAC will primarily fall to the public authorities who implement the technological solutions namely Staffordshire Police and Staffordshire County Council respectively.

6.7 **Agency representatives**: -

- Agree to work with partners in a locality relating to M.A.R.A.C. cases.
- Ensure information presented to M.A.R.A.C. conforms to the principles of data protection.
- Ensure that any actions issued by the M.A.R.A.C. are completed within the agreed time frames.
- To continue to communicate and update partners and the case coordinator of any relevant information linked to the M.A.R.A.C. case thereafter.

7 Information security

7.1.1 This is vital, therefore personal data must not be forwarded by post nor will documentation be printed.

7.1.2 A response to a request for information will be expedited within a reasonable period.

7.1.3 Information will be shared via the declared media type for each meeting forum. All necessary security requirements will be applied by the strategic theme owner of Staffordshire Police as the lead agency on behalf of the partnership.

7.1.4 Data subject Access Requests:

7.1.5 All subject access requests will be dealt with by the receiving organisation.

7.1.6 All requests for combined data on a joint system should be referred to Staffordshire County Council Information Governance Unit before any further action is taken. Any other requests for combined data should be directed to Staffordshire Police.

8 Review

8.1.1 The agreement will be reviewed as required by the Domestic Abuse Commissioning and Development Board. Any amendments as identified by any partner in the interim period, will be made as soon as is reasonably practicable and can be forwarded to the MASH Principal Officer in the first instance until such other arrangements come into force.

9. Complaints

9.1 Any complaints made with regard to the disclosure of information will be directed to the agency concerned. Complaints will be dealt with in accordance to the internal complaints procedure of that agency, but any issue that is to be referred to the supervisory authority should be notified to all agency Information Governance leads.

9.2.1 Agencies must be aware of the seriousness and consequences of breaching the Information Sharing Agreement regarding disclosure procedures, related legislation and the subsequent impact to the victim and their family, and to other agencies supporting M.A.R.A.C. In any case any personal data breach shall without undue delay and where feasible, not later than 72 hours after becoming aware of it, notify the breach to the supervisory authority unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Notwithstanding this controllers should take mitigating action where possible.

9.2.2 Please note breaches of data protection carry significant penalties and the supervisory authority treat public authorities no differently to all others.

10. Signatories

10.1 All partners must be a signatory to the One Staffordshire Information Sharing Protocol and also to this agreement to ensure the integrity of the process.

Staffordshire County Council

Name: _____

Position: _____

Signature:_____

Staffordshire Police

Name: _____

Position: _____

Signature:_____

Local Govt

Name: _____

Position: _____

Signature:_____

Housing

Name: _____

Position: _____

Signature:_____

Partner

Name: _____

Position: _____

Signature:_____

Partner

Name: _____

Position: _____

Signature:_____

Staffordshire Fire and Rescue

Name: _____

Position: _____

Signature:_____

Partner

Name: _____

Position: _____

Signature:_____

Partner
Name: _____

Position: _____

Signature:_____

Partner
Name: _____

Position: _____

Signature:_____

Appendix A

Restricted when completed
MARAC confidentiality statement

MARAC name		Date of MARAC	

The chair of the meeting reminds all concerned of the principles within the MARAC Information Sharing Agreement

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

All agencies should ensure that all minutes and related documentation 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 age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.

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

By signing this document we agree to abide to these principles.

Restricted when completed

MARAC confidentiality statement continued (attendees)

MARAC name		Date of MARAC	

Agency	Name of Representative	Signature	Email

Appendix B
1

Legislation Summary and Guidance

Introduction

Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function.

In many instances legislation tends to use broad or vague statements when it comes to sharing personal information i.e. 'the agency is required to communicate…', or 'will cooperate with...', without actually specifying exactly how this may be done. This is because legislation that specifically deals with the use of personal information already exists; namely, the Data Protection Act and General Data Protection Regulation; in most cases links into most other legislation.

Data Protection legislation sets out to govern the collection, use, storage, destruction and protection of a living person's personal data. It does not set out to prevent the sharing of personal information. To the contrary, provided that necessary conditions are met, sharing is perfectly legal.

Legislation covered in this appendix:

- Data Protection Act 2018
- General Data Protection Regulation
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Digital Economy Act 2017
- Crime and Disorder Act 1998
- The Police and Justice Act 2006
- Statutory Instruments 2007 No. 1831 the Crime and Disorder (Prescribed Information) Regulations 2007
- Statutory Instrument 2007 No. 1830 the Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007
- Anti-Social Behaviour, Crime and Policing Act 2014
- Regulation of Investigatory Powers Act 2000
- Access to Health Records Act 1990
- The Freedom of Information Act 2000
- The Local Government Act 1972
- Localism Act 2011
- Immigration and Asylum Act 1999
- Criminal Justice Act 2003
- The Children Act 1989
- The Children Act 2004
- Children (Leaving Care) Act 2000
- Protection of Children Act 1999
- Education Act 1996

- Education Act 2002
- Education (SEN) Regulations 2001
- Learning and Skills Act 2000
- National Health Service Act 1977
- Health Act 1999
- National Health Service and Community Care Act 1990
- National Health Service Act 2006
- Care Act 2015
- National Audit Act 1983
- Civil Contingencies Act 2004
- Caldicott

Appendix B 2

- Mental Capacity Act 2005 Code of Practice
- Every Child Matters (ECM) Initiative
- Safeguarding