Domestic Abuse MARAC

Victoria Blyth	19/08/2021

Process or Project

Description of the planned activity

There is multiple legislation that covers the work of managing and reducing domestic abuse, including the recent Domestic Abuse Act 2021 (DAA).

- **Section 1: Definition of "domestic abuse" for the purpose of the DAA**

(1) The behaviour of a person ("A") towards another person ("B") is "domestic abuse" if—
(a)A and B are each aged 16 or over and are personally connected to each other, and
(b)the behaviour is abusive.
(2) The behaviour is "abusive" if it consists of any of the following—
(a)physical or sexual abuse;
(b)violent or threatening behaviour;
(c)controlling or coercive behaviour;
(d)economic abuse (see subsection (3 below));
(e)psychological, emotional or other abuse;
and it does not matter whether the behaviour consists of a single incident or a course of conduct.
(3)"Economic abuse" means any behaviour that has a substantial adverse effect on B's ability to—
(a)acquire, use or maintain money or other property, or
(b)obtain goods or services.
(4)For the purposes of this Act A's behaviour may be behaviour "towards" B despite the fact that it consists of conduct directed at another person (for example, B's child).
(5)For the meaning of "personally connected", see section 2.

- **Section 2 Definition of "personally connected"**

(1)For the purposes of this Act, two people are "personally connected" to each other if any of the following applies—
(a)they are, or have been, married to each other;
(b)they are, or have been, civil partners of each other;
(c)they have agreed to marry one another (whether or not the agreement has been terminated);
(d)they have entered into a civil partnership agreement (whether or not the agreement has been terminated);
(e)they are, or have been, in an intimate personal relationship with each other;
(f)they each have, or there has been a time when they each have had, a parental relationship in relation to the same child (see subsection (2));
(g)they are relatives.
(2)For the purposes of subsection (1)(f) a person has a parental relationship in relation to a child if—
(a)the person is a parent of the child, or
(b)the person has parental responsibility for the child.
(3)In this section—

"child" means a person under the age of 18 years;
"civil partnership agreement" has the meaning given by section 73 of the Civil Partnership Act 2004;
"parental responsibility" has the same meaning as in the Children Act 1989 (see section 3 of that Act);
"relative" has the meaning given by section 63(1) of the Family Law Act 1996.

- **Section 3 Children as victims of domestic abuse**

(1)This section applies where behaviour of a person ("A") towards another person ("B") is domestic abuse.
(2)Any reference in this Act to a victim of domestic abuse includes a reference to a child who—
(a)sees or hears, or experiences the effects of, the abuse, and
(b)is related to A or B.
(3)A child is related to a person for the purposes of subsection (2) if—
(a)the person is a parent of, or has parental responsibility for, the child, or
(b)the child and the person are relatives.
(4)In this section—
"child" means a person under the age of 18 years;
"parental responsibility" has the same meaning as in the Children Act 1989 (see section 3 of that Act);
"relative" has the meaning given by section 63(1) of the Family Law Act 1996.

To meet the full range of social, welfare, economic, safety, accommodation, criminal and civil justice needs that individuals living with, escaping, or committing domestic abuse have, a multi-agency partnership approach is required. This helps to deliver the best safeguarding decisions that are timely, necessary and proportionate interventions. Decision makers need the full information picture concerning an individual and their circumstances to be available to them. 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.

Domestic Abuse Multi-Agency Risk Assessment Conferences (MARAC) in each borough are a key part of the DA work. A MARAC is a meeting where information is shared on the highest risk domestic abuse cases between representatives of local authorities, the police, probation, health and mental health, education, drug and alcohol services, charities, housing practitioners, Independent Domestic Violence Advisers (IDVAs), and other specialists from the statutory and voluntary sectors. After sharing all relevant information about a victim, the representatives discuss options for increasing the safety of the victim and turn these into a co-ordinated action plan.

Is the processing novel or has anything similar been undertaken before? Will you be using any innovative technical or organisational solutions, like smart tech?

The collection and sharing of data surrounding Domestic Abuse Support is not a new activity and existing legislative requirements cover the arrangements for doing so.

Will you use systematic and extensive profiling or automated decisions to make significant decisions about people? Will you use profiling, automated decision making or special

category data to make decisions about someone's access to a service, opportunity or benefit?

Each Domestic Abuse referral will discuss individuals, children, young people, and families.

Information collated from the agencies involved will be assessed to determine the best plan to improve outcomes. This will include whether an individual gains access to a range of services. This will include significant amounts of special category data and criminal data.

Do you plan to combine, compare or match data from multiple sources *eg fraud prevention*?

Yes, depending on the circumstances of the service user, including (but not exhaustive) local authorities, the police, probation, health and mental health, education, drug and alcohol services, charities, housing practitioners, Independent Domestic Violence Advisers (IDVAs), and other specialists from the statutory and voluntary sectors.

In order for Domestic Abuse services to be effective, it is necessary for all relevant personal, sensitive and special data to be shared regarding the individual(s) from all agencies/partners who are involved with the referral.

Data will be shared and matched to assess level of risk, and to identify and provide suitable intervention.

Will you process personal data in a way that involves tracking individuals' online or offline location or behaviour eg vehicle tracking or monitoring an individual's social media?

No

Anticipated start data and duration of processing (ongoing if no set end date)

Ongoing

Purpose & Benefits

What are the aims of the processing? What is the intended effect on individuals?

The primary focus of the MARAC is to safeguard adult victims age 16 and above and any dependents at risk of harm, and manage the behaviour of those who commit abuse.

The data sharing in the MARAC context helps organisations to meet their responsibilities for:

- Identifying individuals at risk.
- Providing advocacy to victims.
- Providing refuge to victims, including sanctuary schemes aimed to support a victim feeling safe in their home.
- Supporting and protecting witnesses.
- Minimising risk of harm and improving the well-being of victims.
- Investigating and prosecuting those who commit abuse.

- 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.
- Delivering a safe environment overall for the public.

Why are you planning to undertake this processing? What legislation requires/affects your processing?

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. These agencies are local authorities, the police, probation, health and mental health, education, drug and alcohol services, charities, housing practitioners, Independent Domestic Violence Advisers (IDVAs), and other specialists from the statutory and voluntary sectors.

The Crime and Disorder Act 1998 places this obligation on a statutory footing, requiring some organisations to form partnerships to tackle crime and disorder, including domestic violence, and provides a legal power to share information.
The Domestic Abuse Act 2021 provides further protections to the millions of people who experience domestic abuse, as well as strengthen measures to tackle perpetrators. Detailed factsheets on each new measure are available on gov.uk.
The Domestic Abuse Act:

- creates a statutory definition of domestic abuse, emphasising that domestic abuse is not just physical violence, but can also be emotional, coercive or controlling, and economic abuse. As part of this definition, children will be explicitly recognised as victims if they see, hear or otherwise experience the effects of abuse;
- creates a new offence of non-fatal strangulation;
- extends the controlling or coercive behaviour offence to cover post-separation abuse;

Articles 2 and 3 of the Human Rights Act 1998 (HRA) place an obligation on public authorities to protect people's right to life and their right to freedom from torture and inhuman and degrading treatment. Meeting these obligations may necessitate lawful information sharing and the processing of personal data.

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 C – 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);

Whilst we work collaboratively with individuals, consent is not a lawful basis for processing, including for referrals.

What are the benefits to the individual, society and the organisation(s) involved?

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.
- 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.

What geographical area will the processing cover? *(This would generally be Barnet only, but your work may involve pan-London or national projects*)

The service delivery will take place in London, and organisations have different boundaries within London, such as local authorities, police BCUs (Borough Command Units) and CCGs. Data will be processed in relation to individuals anywhere in the UK. This includes the placement of victims from one council area into another area, which is a regular activity.

Agencies may receive or share data outside the UK if required for safeguarding or for the prevention and detection of crime. This might be necessary in relation to Forced Marriage, Honour Based Abuse, Female Genital Mutilation, or other domestic abuse crimes.

Individuals (data subjects)

What types of data subjects are involved? Tick all that apply.

☒ Customers or Service users
☒ Service providers / Contractors
☐ Residents
☐ Complainants
☐ Claimants
☐ Recipient of benefits
☒ Volunteers
☐ Traders or people subject to inspection
☐ People captured on CCTV
☒ Representative of another organisation
☐ Licence and permit holders
☒ Employees (previous or current)
☐ Councillors, MPs, elected officials
☒ Professional adviser or consultant (e.g., doctor or lawyer)

☐ Any

Are the data subjects considered vulnerable eg children or domestic abuse victims? What is the council's relationship with the data subject? Is there an imbalance of power, as with employees? How much control will data subjects have?

Yes - Victims of domestic abuse are vulnerable and include children. Witnesses and perpetrators can also be vulnerable.

Victims, witnesses and perpetrators have very little control over the processing of their personal data, and the council, its contractors and partners, are in a position of power over data subjects because of the wide-ranging powers of the local authority and other relevant public bodies to take significant action toward and for individuals for safeguarding purposes.

Expected volume of data subjects *eg number of people or number of records*

An average of 400-600 victims, their family members, and corresponding perpetrators, per MARAC, per year. Multiple records relating to one case.

How is the individual being informed of the processing *(privacy notices)*? Do you plan to process personal data without providing a privacy notice *eg investigations or covert surveillance*?

Due to the nature of the work, which can involve investigation prior to engaging directly with data subjects, it is not always possible to provide a privacy notice directly to data subjects at the beginning. Data subjects who are previously convicted or alleged perpetrators may not receive privacy information, under the crime prevention exemption.

It can reasonably be assumed that data subjects expect that personal data will be processed and shared for criminal investigation and prosecution.

Each organisation will have suitable published privacy notices that describes the work we do to safeguard children and adults and prevent crime, and this included MARAC sharing.

In one to one support with victims and witnesses, the Domestic Abuse services and MARAC work are described to data subjects and the possible outcomes are explained. This includes information provided to children in language suitable for their age. Families are also advised of processes, rights and information sharing.

How do you plan to support the Rights of Data Subjects (*eg access to information*)?

Privacy information is published and otherwise made available to data subjects.

Each organisation will have processes for responding to data subject requests – there may be exemptions, where complying with the request may hinder investigations or place individuals at risk of harm.

Will your processing prevent individuals from exercising a right, or using a service or contract?

Processing may lead to convictions and a prison sentence for perpetrators.

Data

What type of information will be collected? Tick all that apply.

☒ Name
☒ Address

☒ Contact details
☒ DOB
☒ Equalities information
☒ Financial information
☐ Property information
☒ Criminal (allegation or prosecution) information
☒ Health / Medical information
☒ NHS number
☒ Support network

☒ Social services information
☐ Human Resources information

☒ Employment
☒ Education information
☒ Housing information
☒ Family / relationship information
☒ Information from another local authority
☒ Images in photographs, film or CCTV

☒ Referral / Assessment information
☐ Referees

Are you processing?

☒ Special category data

☒ Criminal / allegation offence data

Please specify.

Special category and criminal data includes:

- Sexual Orientation
- Religion
- Ethnicity
- Physical Health – including evidence of abuse
- Mental Health – including evidence of abuse
- Commission or alleged commission of a crime and any convictions

High volume of special category data in relation to health, gender, sexuality, race, ethnicity, religion and other equalities information. This information is essential in order to categorise and define areas of need and risk in the community and support vulnerable individuals more effectively.

Criminal data will be processed on a large scale and data processing for law enforcement purposes will also take place.

Will you be processing biometric data? Please specify.

The police and Probation Service will process biometric data, but this is not expected to be shared within the MARAC.

Will you be using the above special category, biometric or criminal data on a large scale? Please specify.

Yes.

Is there a risk of physical harm in the event of a security breach *eg fraud investigations or child exploitation*?

The personal data involved is highly sensitive and there are significant risks to safety and well-being if the information is shared or disclosed improperly. In general, there is a high risk to individuals in relation to a breach of information security as victims or witnesses may be placed at risk of further abuse. There may also be harm to perpetrators in the event of a breach.

How is the information being collected? Where are you getting it from?

Data each organisation holds, to be shared at MARAC, will originally come from a wide variety of sources of data, including from data subjects themselves.

The information is collected by those organisations/people who have a contribution to make due to their knowledge of the data subject(s), or their expertise relevant to the case. This is likely to include:

- Victims
- Witnesses

- Parents / those with parental responsibility if child involved
- Family members (including the wider family)
- Foster carers (current or former)
- Perpetrators
- Residential care staff
- Social work and health care professionals
- Probation or the Youth Offending Team
- Local authority housing services
- IDVA or similar supporter / advocate
- Investigators
- Police National Computer data, CRIS, Crimint, Merlin, 124D (domestic violence notebook), Part 2 Risk Assessments
- Involved third sector organisations, eg substance misuse support services
- Alcohol and substance abuse services
- A representative of the armed services, in cases where there is a service connection
- Any other relevant professional or service provider

Are you processing personal data for a different purpose than it was originally collected?

No

Volume of data *e.g., number of records*?

An average of 400-600 victims, their family members, and corresponding perpetrators, per MARAC, per year. Multiple records relating to one case.

How often will you be using the data *eg every day or annually*?

Every day.

How is the information being stored, including backups, paper files in off-site storage, copies etc?

Organisations must keep data on suitably secure and encrypted networks and kit. Minimal paper records are used, and these are stored and transported securely.

Data is generally transferred between agencies by secure data transfer (email or portal).

Organisational Security:

- Mandatory DP training is in place for all staff
- Appropriate written guidance is in place - Relevant staff have been trained and are familiar with the written guidance.
- Physical security measures have been identified (e.g., building access, locked down areas controlled by ID card, lockable cupboards for sensitive data, secure printing, secure shredding)
- Paper copies are kept to a minimum.

Technical Security

- All laptops are encrypted and complex passwords used
- Data encrypted in transit – whether this is by email, or on removable media

How will you ensure good data quality? *eg regular checks or updating processes*

All agencies are expected to have suitable processes to manage data quality. There are also checks and balances through the safeguarding process which ensures the information held is accurate.

What processes are/will be in place for editing or deleting information? We must be able to amend and fully delete personal data from systems.

All agencies are expected to have suitable processes to manage secure editing and deleting of data. Retention periods are set and there is a process for deletion of electronic and any archived paper records when the retention period is reached.

- **Are you using contractors/service providers to process the data?**

Yes. The local authorities often employ contractors for MARAC administration, IDVA service, advocacy and refuge services. These contractors are usually data controllers, as well as the council, because of the independence they have in processing the personal data for delivering these services. These contracted organisations attend and share data within MARAC, as relevant to the case at hand.

Organisations may use contractors for case management systems.

How is the information to be transported/transferred *(electronic and paper)*?

Data will be shared using secure email or secure sharing platforms.

Minimal paper records are used, and these are only transported when necessary.

How will access to the data be managed and monitored *eg audit trails, logs*? Which officers/roles will have access to the asset?

All agencies are expected to have audit trails on their networks/systems. User security roles will be clearly defined with controlled access rights and audits of users.

MARAC documents are shared by the author agency prior to the meeting. All paper copies of documents are collected at the end of meeting, counted and removed by staff for secure destruction.

What security measures will be in place?

- Access controls and audit trails for electronic systems
- Data owners identified and understand their responsibilities
- Appropriate written guidance is in place
- Relevant staff have been trained and are familiar with the written guidance; and other partners understand their electronic and paper access only permits reading of relevant records
- Physical security measures have been identified (e.g., building access, locked down areas controlled by ID card, lockable cupboards for sensitive data, secure printing, secure shredding)

- Where a third party is engaged, a written, signed contract is in place

Auditing of organisational measures is planned, to ensure compliance and efficacy.

Are there are plans to store data outside the UK? Consider hosted sites, disaster recovery and IT support.

Each agency must ensure that appropriate written agreements and risk assessments are in place for any outside UK data processing.

Data may be received or shared outside the UK if required for safeguarding or for the prevention and detection of crime. This might be necessary in relation to Forced Marriage, Honour Based Abuse, Female Genital Mutilation, or other domestic abuse crimes.

Will reports be generated from this information, or statutory returns? If so, will the information be personally identifiable or anonymous?

All statutory returns and internal audit reports anonymised.

What is the retention period for this information? Consult the council's Retention Schedule.

Each agency must ensure suitable retention periods are set, and adhered to.

What process is/will be in place to implement this retention period?

Will be different for each organisation.

If the organisation/service ceases, what will happen to the information?

It is not expected that domestic abuse support services will cease.

Can data be anonymised or pseudonymised? How will ensure you only use the minimum amount of data required to complete the aim?

Information can be pseudonymised for some data research and reporting purposes.

Who do you plan to share information with? Tick all that apply

☒ DWP ☐ Ofsted

☒ Local authorities
☒ Legal representatives
☒ Police
☒ Health agencies
☒ Judicial agencies eg Courts
☒ Voluntary agencies / Third sector
☒ Housing providers
☒ Expert witnesses
☒ Prison / Probation services

What information is shared?

Any data relating to the case will be shared between the organisations taking part in MARAC.

Risks

Are there any known information risks, issues or public concerns? Has there been press interest or court cases relating to this type of processing?

Known high risk processing. There is high public concern and interest in the effective management of domestic abuse support services, both to keep data confidential, but also to share it efficiently when needed to avoid serious risk to an individual.

Risk Table

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
Separation of functions as so many different partners and agencies involved could cause delay of delivery through ineffective communication. Failure to provide high quality support and solution services may result in detrimental impact to those in need	Possible	Severe	High	Effective information sharing agreements and close working relationships between LBB, partners, agencies and other relevant parties are in place. Written procedures and training for staff to ensure suitable and timely data sharing for safeguarding.	Reduced	Medium	Yes
Inappropriate sharing of confidential information.	Possible	Severe	High	Effective training in place and all parties trained and reminded regularly about data sharing and security. Written procedures.	Reduced	Medium	Yes
Loss of data in transfer, either poor information security or malicious attempt.	Possible	Severe	High	Appropriate technical and organisational measures in place and staff trained to follow their organisational policies and procedures for transfer and transport of personal data, with encrypted electronic documents	Reduced	Medium	Yes

				expected to be used in most cases.			
Loss of data or availability of data; through poor security measures and/or malicious attempt.	Possible	Severe	High	Appropriate technical and organisational measures in place and staff trained to follow their organisational policies and procedures. Strong data security measures, controlled access, audit trails.	Reduced	Low	Yes

Approval

DPO advice provided by:	Victoria Blyth	Date:
DPO advice: The risks are considered acceptably mitigated for this area of work which is regulated by statutory provisions and provides a valuable public service.		
IAO agreement		If your decision departs from DPO views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Date review to take place:	Date Agreed: