COMMUNITY RISK MARAC
INFORMATION SHARING AGREEMENT

London Borough of Islington
The Metropolitan Police Service
Partners for Improvement
Registered Housing Providers
Victim and Witness Support
Mental Health Services

[Blank Page]

Document History

This document has been distributed to:

Version	Date	Author	Released to	Comments
First draft	09/04/2014	Sinead Hayden	Alison Blackburn and Keith Stanger	First draft for consultation and ratification

This document requires the following approvals

Date	Version	Name	Role
April 2014	V1	Community Risk MARAC	Owner of agreement and process.

[Blank Page]

TABLE OF CONTENTS

1. PURPOSE OF THE AGREEMENT

The purpose of this Information Sharing Agreement is to provide a robust framework for the legal, secure and confidential sharing of personal information between the agencies listed in Section 5 'The Agreement'.

This agreement has been developed to:

a) Define the specific purposes for which the signatory agencies have agreed to share information.

b) Describe the roles and structures that will support the exchange of information between the signatories.

c) Set out the legal gateway through which the information is shared, including reference to the Human Rights Act 1998 and the common law duty of confidentiality.

d) Describe the security procedures necessary to ensure compliance with responsibilities under the Data Protection Act and agency specific requirements.

e) Describe how this arrangement will be monitored and reviewed.

It is the purpose of this Agreement to clarify the understanding between signatories and each party's responsibilities and duties towards each other, to be fully aware of the process for information exchange and will comply with all legal requirements.

The signatories to this agreement will represent the following agencies/bodies:

Please refer to page 19 for list of organisations.

2. SPECIFIC PURPOSE FOR SHARING INFORMATION

The purpose of this information sharing agreement is to facilitate the lawful exchange of personal and sensitive information, in any form, for notified and defined purposes. The collection of information will form the basis of

- Managing the risk of those identified as vulnerable individuals to increase safety, health and well-being of victims and/or witnesses, both adults and children
- Tackling the Anti-Social Behaviour (ASB) of perpetrators, identify groups or individuals with the greatest need for intervention.
- Ensure multi-agency working and multi-agency effective communication

2.1 Management Summary

Signatories to this agreement have a responsibility to share information and work together with the aim of reducing crime, ASB and victimisation, and ensuring community safety in the London Borough of Islington.

The purpose of this agreement is to provide a process and mechanism whereby information relating to individuals and/or groups can be shared to aid and assist the working practices and objectives of all organisations.

The information collected will be recorded and discussed within the Community Risk MARAC and will form the basis of supporting the management of risk to vulnerable people and subsequent prevention of crime and disorder.

The information held will be personal and sensitive data, including names, addresses and histories of individual's criminal activities and that of other household members, and/or status as a tenant or resident of Islington Borough.

The agreement will therefore allow data to be shared for the purpose of: -

- The identification and prioritisation of vulnerable individuals, both victims and perpetrators of ASB;
- The identification of safeguarding issues relating to these individuals, increasing safety, health and wellbeing;
- Partnership problem-solving approaches to tackling issues of managing the risk of vulnerable of victims and reducing repeat victimisation;
- Identifying gaps in provision and recommending projects and approaches to tackle antisocial behaviour in Islington.
- Improving agency accountability and improving support for staff involved in cases;
- Construct jointly and implement a risk management plan that provides support to those at risk of harm

Information derived from all sources will be assessed for its reliability and validity to ensure meaningful conclusions can be drawn. It will also be used to assist with evidence gathering to enable appropriate support for residents and vulnerable victims, as well as ASB interventions to take place, including tenancy action.

2.2 Objectives

What are the objectives of the project?

The Safer Islington Partnership has a commitment to ensure Islington residents experience a peaceful and enjoyable existence in their home and surrounding area. Successfully sharing information with authorised parties can contribute to the strategic aims and objectives of the Safer Islington Partnership.

By providing each organisation with access to up to date robust managerial information, the capacity to identify required interventions or appropriate support / enforcement actions and formulate action plans will be enhanced. The sharing of information will increase awareness of issues that may have previously been managed in isolation by a party or by an additional 3rd party organisation.

Partner Agency Benefits

Most information and data exists in isolation and cannot be intelligently interrogated with other information sources.

This agreement provides legal clarity for all staff within each organisation about information sharing. This will enable all organisations to feel confident that they can share information in a way that is comprehensible and secure within the legal framework.

By promoting a greater flow of information between agencies there can be better planning and targeting in service delivery.

The sharing of information between agencies can promote the safety of clients, staff and the public, for instance by highlighting areas of concern across organisations rather than restricting them to the agency where the concern originated.

The promotion of information sharing between agencies can lead to less duplication of work.

The agreement will foster better working relationships and understanding of all partner's issues and constraints of their work.

The agreement will serve to increase and enhance each partner's awareness of the tools available to use in their day to day role, which will improve partnership working.

Citizen Benefits

The sharing of information will benefit the community on the following levels: -

- Faster identification of issues that may be impacting the community.
- Increase the safety, health and well-being of victims and / or witnesses.
- Reducing repeat victimisation.
- Provide a more dynamic and proactive approach to tackling issues and delivering appropriate enforcement and provision of interventions including support.
- Addressing perpetrators behaviour through co-ordinated action.

How will this information sharing arrangement further those objectives?

a) Sharing information will enhance the appropriateness of interventions and enforcement/support actions by ensuring that data and information is not used in isolation.
b) The identification of individuals at risk, repeat callers and vulnerable victims will subsequently enable agencies to apply the required or necessary support
c) The quality of the inferences will be enhanced by agencies sharing appropriate data set within a clear framework.

2.3 Information to be shared

The following information will be shared:
Shared information will include personal data and sensitive personal data (as defined in the Data Protection Act 1998) held by the signatory agencies about people that is relevant and supports the stated objectives of the Safer Islington Partnership.

Personal data:

Data which relates to an individual who can be identified from that data or any other information held or likely to be held.

Sensitive personal data:

Personal data which consists of information concerning racial or ethnic origin, political opinions, religious or other similar beliefs, physical/mental health or conditions. Sexual life, alleged or committed offences, proceedings, disposal or sentence concerning any alleged or committed offences (Information Commissioner's Office [2001].

For a full specific list of information to be shared please see Appendix A. For definition of terms refer to Appendix B.

3. LEGAL BASIS FOR SHARING

Any processing of personal data must generally (there are certain limited exceptions) comply with the Data Protection Principles set out in Schedule 1 of the Data Protection Act 1998 ("DPA"):

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
   (a) At least one of the conditions in Schedule 2 is met, and
   (b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Crime and Disorder Act 1998, section 115, provides the power to exchange information between partners where disclosure is necessary **or expedient** to support local community safety strategy or other provisions in the Crime and Disorder Act. This provision makes the processing of data for the purposes of this agreement lawful and in compliance with the 1st Principal.

Full compliance with the DPA must be ensured when sharing personal data or sensitive personal data.

The Conditions in the DPA allowing the sharing of personal data are set out in Schedule 2. At least one Condition must be met:

http://www.legislation.gov.uk/ukpga/1998/29/schedule/2

The **relevant** provisions (irrelevant provisions omitted) for information sharing under this agreement are:

"1 The data subject has given his consent to the processing.

…

3 The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary—

(a) For the administration of justice,

…

(b) For the exercise of any functions conferred on any person by or under any enactment,

…

(d) For the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

Condition 5 is most likely to apply to personal data exchanged hereunder. Consent would likely only be given by complainants, not the subjects of those complaints.

When sharing sensitive personal data, at least one of the Conditions in Schedule 3 must be met as well as at least one of the Conditions in Schedule 2. The relevant Schedule 3 Conditions are:

*"1 The data subject has given his **explicit** consent to the processing of the personal data.*

3 The processing is necessary—

(a) In order to protect the vital interests of the data subject or another person, in a case where—

(i) Consent cannot be given by or on behalf of the data subject, or

(ii) The data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) In order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

6 The processing—

(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or

(c) Is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7(1) The processing is necessary—

(a) For the administration of justice,

(b) For the exercise of any functions conferred on any person by or under an enactment, or

9(1) The processing—

(a) is of sensitive personal data consisting of information as to racial or ethnic origin,

(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

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

Of these, Conditions 6 and 7(1)(b) are most likely to apply to sensitive personal data exchanged hereunder. Condition 9 might be relevant for equality impact assessments and other statistical purposes. In respect of consent, this must be explicit, not implied i.e. the data subject must give informed and unambiguous consent by e.g. signing a declaration as to the use his/her personal data will be put.

Human Rights - Article 8: The Right To Respect For Private And Family Life, Home And Correspondence

a) Everyone has the right to respect for his private and family life, his home and his correspondence.

b) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

To the extent that data sharing for the purposes of this agreement is necessary for the processing of crime and disorder interventions which in turn are necessary for the purposes of public safety, the prevention of disorder or crime, or the protection of the rights and freedoms of others, then such data sharing comes under Article 8(b) and is not in breach of the Article 8(a) right.

Any enquires on these acts should be directed to:-

LBI - Michael Smith Email: mike.smith@islington.gov.uk

4. DESCRIPTION OF ARRANGEMENTS INCLUDING SECURITY MATTERS

4.1 DESIGNATED LIAISON OFFICERS

The Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007 sets out a statutory requirement for each responsible authority to nominate a designated liaison officer (DLO) whose role will be to facilitate the sharing of information with other partners.

The DLO, whose role includes sharing information with partners, should allow other agencies to know who to approach first for information. The DLO should be a source of expertise allowing good quality decisions about information sharing to be made.

Other responsibilities of the DLO's will be when sharing information:

- To act as the single point of contact for information requests between the partnership and relevant organisations,
- Understand the relevant legislation.
- Work with other DLOs to establish the best ways to share information.
- Act as the first point of call for any technical problems with sharing the information that may arise.

Each partner will also appoint a Primary Designated Officer (PDO) who will be a manager of sufficient standing and have a co-ordinating and authorising role.

Specific responsibilities of the PDO's will be:

- Ensuring that all DLOs and other staff are fully aware of their responsibilities.
- Appointing other staff in the agency to act as DLOs in their absence.
- Authorising the agency involvement and co-operation in the information sharing process at every stage.
- Keeping a Protocol Folder which holds all the partners information sharing documents in general.
- Ensuring the agency's Data Protection Notification entry is accurate, up to date and adequate for the task

The PDO or DLO are the data owners. As such, any final decision on whether to share sensitive information rests with them.

<u>Only DLOs and PDOs can make formal requests and document agreements for the sharing of personal information.</u>

It is the responsibility of the DLO and PDO to ensure the processing of the personal data held is in keeping with the Data Protection Act 1998

By declaring a commitment to the procedures set out in this protocol, signatories will ensure that data sharing arrangements between them take account of the following legislation:

i. Data Protection Act 1998, for the processing of personal Information;

ii. Crime and Disorder Act 1998, Section 115, provides the power to exchange information between partners where disclosure is necessary to support local Community Safety Strategy or other provisions in the Crime and Disorder Act

iii. The Human Rights Act 1998, for the individual's right to privacy.

Agencies also agree to ensure their actions are in compliance with any other relevant legislation, such as:

i. - Common law duty of confidence;

ii. - Freedom of Information Act 2000;

iii. - Housing Act 1996, for Registered Social Landlords;

iv. - Mental Health Act 1983, for the health sector;

v. - Health and Social Care Act 2001, for health and social services;

vi. - Education Act 1996;

vii. - Confidentiality NHS code of practice

viii. - The NHS care record Guarantee for England

ix. - The Social Care record Guarantee for England

x. - The International information security standard ISO /IEC 27002:2005

xi. - The information Security NHS code of practice

xii. - The records management NHS code of practice

4.2 SENDING / SHARING INFORMATION

Referral and Information request process

Referrals to the Community Risk MARAC should be made by means of completing of the referral form, an example of which can be found in 'Appendix C – Referral Form'. Once completed, this form will become a RESTRICTED document. The form should be sent via secure email to the Community Rick MARAC Administrator. The Community Risk MARAC Administrator will securely request further information to support the application.

Information to be shared

Information that is provided and shared within this Agreement will include Non Personal data, Depersonalised Data, Personal Data, and Sensitive Personal Data (as defined in the Data Protection Act).

For a list of data please see 'Appendix A – Information to be Shared'. This is not an exhaustive list and may be added to as required,

How information will be shared

When sharing information between signatory parties only information that qualifies as 'need to know' should be derived and shared. Fact (based on data) and opinion should be distinguished. Collated information should be shared electronically via secure email. If a copy of an existing document is required this should be scanned and emailed securely. Emails containing data should only be sent to named individuals and not to generic email inbox addresses. By ensuring that all requests and responses for information are recorded electronically an electronic audit trail of information sharing will be created that can be referred to at a later date if the need arises.

How shared information will be used

Information will be used to fulfil the objectives of either/each organisation. This will include but not be restricted to:

- Use in application of legal enforcement;
- Improve the safety, health and wellbeing of referred victims and witnesses;
- Risk management and reduce victimisation;
- Multi-agency problem-solving;
- Tenancy management including resident liaison, intelligence gathering and victim support;

4.3 DATA TRANSPORT

Internal Islington Council transfer

Personally identifiable data following a referral will be stored in a secure area on the council network. Where necessary, data may be securely emailed within the council (@islington.gov.uk accounts). Data must only be emailed to a named individual and never to a group account.

Sharing between the council and external agencies

Data containing personally identifiable information or sensitive personal data MUST be sent through secure email. The following forms of secure email may be used:

- Criminal Justice Secure email (CJSM)

CJSM is a government accredited secure route for sending emails to Criminal Justice organisations, including Crown and Magistrates' Courts, Crown Prosecution Service, Police, and the National Offender Management Service.

- Government Secure Intranet (GSi) addresses;

GSi is a UK Government wide area network, whose main purpose is to enable connected organisations to communicate electronically and securely low protective marking levels.

- All other email domain addresses (Not Islington.gov.uk, CJSM, or GSi);

Secure encrypted email MUST be used. Islington council's secure email is Proofpoint, and this must be used when transferred personally identifiable or sensitive personal data.

Where possible electronic mails containing Personal and Sensitive Personal Data should not be sent outside of the networks mentioned above. However if this is not possible, electronic mails should only be sent to addresses which are directly linked to the recipient, under no circumstances should any electronic mail containing Personal data or Sensitive Personal Data be sent to group email addresses, or addresses that have not been verified by the recipient.

In addition, emails will only be sent to recipients who have emails associated with an organisation containing address strings such as gov.uk and nhs.uk and not to personal or social email addresses.

Under no circumstances should Personal or Sensitive Personal Data be included in the Subject, or the Body of any electronic mail that is sent outside of the networks mentioned above. Any Personal Data or Sensitive Personal Data should be contained in a separate document, which is password protected, and attached to the electronic mail.

Sharing data via Removable Media

Personally identifiable data must not be stored on or transported by removable media.

Sharing Data on Paper

It is recommended that all Personal Data and Sensitive Personal Data is transferred electronically. If there is no other option but to print out this data, it is recommended that there is a single point of contact (SPOC) who is responsible for printing this data. Data should not be removed from a secure premises unless absolutely necessary.

Once the Data has been printed, it becomes the responsibility of whoever printed the Data to ensure that Islington's Data Security Procedures are adhered too. Where ever possible, when printing Personal Data and Sensitive Data, the name of the person who is printing the document should be detailed on the print out, desirably in the footer of the document.

4.4 STORING INFORMATION

Data collected electronically by signatories will be stored on secure computer systems that should have security and access protocols in place. Organisations must ensure they have appropriate data storing and sharing mechanisms in place and that staff are appropriately trained.

Data collected in hard copy or paper format will be stored within controlled environments and storage facilities which are secure and alarm protected.

4.5 RECIPIENTS

The recipients of information covered by this agreement will only be those that are signatories to this agreement and those within their organisation who need access to the data for the stated lawful use under either this agreement or the relevant legislation.

4.6 REPORTING DATA BREACHES

A data security breach can happen for a number of reasons:

a) Loss or theft of data or equipment on which data is stored
b) Inappropriate access controls allowing unauthorised use
c) Equipment failure
d) Human error
e) Unforeseen circumstances such as a fire or flood
f) Hacking attack
g) Blagging' offences where information is obtained by deceiving the organisation who holds it

Assessing and reporting a data breach

Islington council's 'Incident Management Policy' specifies the following assessment of each breach, based upon the Information Commissioner's guidance on data security breach management. There may be a requirement to notify the Information Commissioner of any data breach or loss. Any potential breach should be reported to the originating data owner, who will investigate with the council's corporate Information Governance Team.

What happened?

a) Define the type of information lost and number of records.
b) Describe the circumstances of the loss

Containment and recovery

a) Who was involved in the investigation?
b) Who needs to be aware?
c) Can anything be done to recover the loss?

Assessment of on-going risk

a) What type of data is it and how sensitive is it?
b) What harm can be done to the subject?
c) Are there any wider consequences?

Who is the service notifying?

a) Are there any legal requirements?
b) Notifying the parties involved

How will the service ensure this incident does not re-occur?

a) Remedial action already taken
b) Existing policies and procedures in place
c) Conclusion and recommendations

4.7 DISPOSAL OF INFORMATION

Information will be stored in accordance with the operational need of the requesting organisation's operational need and subject to the archiving policy of the supplying organisation. Storage and disposal rules will be agreed between the supplier and the requesting organisations.

5. THE AGREEMENT

The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Ensure appropriate storage and security arrangements are in place and that staff are adequately trained in data handling processes.
- Engage in reviews of this agreement as appropriate.

We the undersigned agree that each agency/organisation that we represent will adopt and adhere to this information sharing agreement:

Agency	Post Held	Name	Signature	Date

Monitoring and review

This agreement will be subject to yearly review to be undertaken within 12 months from the date this standard operating procedure is signed.

The review will be undertaken by members of the Islington Community Risk MARAC under the direction of the Chair.

In the event of any changes or revisions to this agreement being identified prior to this review period then a change request should be submitted to the Community Risk MARAC Administrator to facilitate the document change process.

6. APPENDIX A - INFORMATION TO BE SHARED

Information to be shared should be relevant to the operation requirements of either party. If it includes personal and sensitive information, as covered by schedules 2 and 3 of the Date Protection Act it must meet the provisions of the act and all security protocols.

Examples of personal and sensitive data are listed below;

	Victim	Perpetrator
Demographics	Name	Name
	Date of Birth	Date of Birth
	Gender	Gender
	Address	Address
	Ethnicity	Ethnicity
	Disability	Disability
Children and Family	Name	Name
	Date of Birth	Date of Birth
	Gender	Gender
	Address	Address
	School	School
	Victim Pregnant	Perpetrator Pregnant
Risk Factors	Accommodation	Accommodation
	Substance Misuse / Alcohol	Substance Misuse / Alcohol
	Mental Health needs	Mental Health needs
	Physical Health needs	Physical Health needs
	Repeat reporting / caller	
		Current or previous restrictions / conditions (i.e. ASBOs, non-molestation order)
		Any previous management i.e. IOM
Other	Housing provider	Housing provider
	Housing officer	Housing officer
	Tenancy History	Tenancy History
		Offences committed / alleged offence
	Life style	Life style
	Family and associates	Family and associates
Referee	Name	
	Organisation	
	Telephone / Email	

7. APPENDIX B – DEFINITIONS OF INFORMATION

A. Personal data (defined by the Data Protection Act 1998)
Personal data is any information that either by itself or in combination with other information held or likely to come into the possession of the holder, however recorded, can identify a living individual.

B. Sensitive personal data (defined by the Data Protection Act 1998)
Sensitive personal data is a subset of personal data. It is defined as information describing, in relation to the data subject:
- racial and ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- membership of a trade union;
- physical or mental health condition;
- sexual life;
- commission or alleged commission of any offence; or
- any proceeding for any offence committed or alleged to have been committed by the subject, the disposal of such proceedings or the sentence of any court in such proceedings

In relation to community safety, information that should also be treated as sensitive personal data includes:
- Information relating to victims
- Information relating to witnesses

C. Depersonalised data
(Defined by the Crime and Disorder (Overview and Scrutiny) Regulations 2009)
Depersonalised information refers to information that does not constitute personal data under the Data Protection Act 1998. Depersonalised information can not be used in any way to identify a living individual. No recipient of the depersonalised information should have the ability to 'recreate' certain attributes of the personal data using other information they may be able to access, and hence identify an individual. Depersonalised information is created by 'anonymising' (sometimes also referred to as 'sanitising') personal data. Depersonalised information could include aggregated counts of the number of crimes in a specific area such as a local authority ward, or the original recorded data, albeit stripped of attributes that identify individuals.

D. Protectively marked information
Protectively marked information – Intelligence documents should be marked as 'RESTRICTED' because they contain information that should only be made available to its intended audience, and can only be more widely published with the permission of the supplier from which the information originated. The Protective Marking System (often referred to as the Government Protective Marking System/Scheme or GPMS) is the Government's administrative system to ensure that access to information and other assets is correctly managed and safeguarded to an agreed and proportionate level throughout their lifecycle, including creation, storage, transmission and destruction

8. APPENDIX C – REFERRAL FORM

ISLINGTON COMMUNITY RISK MARAC REFERRAL FORM

REASON FOR REFERRAL – CRITERIA

A: REASON FOR REFERRAL – NEW CASES Please consider the below options as your reason for considering this referral high risk	
1) POTENTIAL ESCALATION OF ASB: There have been a number of incidents by the same perpetrator on the same victim(s) in the last 6 months and they are increasing in severity or frequency:	
2) PROFESSIONAL JUDGEMENT: You as a professional consider the victim/perpetrator to be particularly vulnerable or at risk of serious harm or death.	
3) PERCEPTION **Please take into consideration the victim's own perception of risk and:** **A)** Impairment that may limit mobility or capacity/learning difficulties **B)** Mental health issues **C)** Drug or alcohol misuse **D)** Limited support network	

What is a Community Risk MARAC?

The Islington Community Risk MARAC (Multi-Agency-Risk-Assessment-Conference) is a meeting where information is shared on the highest risk/complex cases between representatives of Community Safety Partnerships Unit, local police, mental health, housing including RPs, floating support, victim support and other specialists from the statutory and voluntary sectors.

After sharing all relevant information they have about a victim /perpetrator, the representatives discuss options for increasing the safety of any victim and turn these into a co-ordinated action plan.

The main focus of the Community Risk MARAC is on managing the risk to the vulnerable victim but in doing this it will also consider other persons affected and managing the behaviour of any perpetrator. The panel will decide on the best approach to managing the overall risk to the victim/the community at large and on effective safety planning strategies.

Information shared at the Community Risk MARAC is confidential and is only used for the purpose of reducing the risk of harm to those at risk.

The Community Risk MARAC is not an agency and does not have a case management function. A lead officer for each case will be nominated at the meeting. **The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the Community Risk MARAC.**

Who should be referred?

A victim /perpetrator should be referred if they are vulnerable or at risk to either themselves or others. The case may be complex or involve a multi-agency approach. The case may be unusual and will not fall under the responsibility of another panel.

COMPLETED FORMS TO COMMUNITY SAFETY PARTNERSHIPS UNIT: by secure email: If you do not have access to secure email refer via your Department's lead officer on the Community Risk MARAC. **Please also send a copy of completed forms to your Agency's Community Risk MARAC rep.** If you are unsure who this is contact Tracy Duligall on- Tel: 020 7527 4125

All referrals sent to CSPU.team@islington.gov.uk **Where possible please use a password protected pathway**

Victim details				
Name (include any aliases)				
Date of birth				
Male / female / transgender				
Address (& landlord if known)				
Ethnicity				
Is the behaviour/actions perceived to be Hate Crime?				
Do they have a Disability (Defined by the Disability Discrimination Act (DDA) *"a disabled person is someone who has a physical or mental impairment that has a substantial and long-term adverse effect on his or her ability to carry out normal day-to-day activities.')*				
Consent given for a support service to contact the victim?				
Is it safe to contact the victim? (N) If Yes please include safe contact details (e.g. mobile/ email & any specific hours to contact)				
Perpetrator(s) of abuse details				
Name(s) (include any aliases)				
Date(s) of birth				
Male / female / trans*				
Relationship to Victim				
Address (& landlord if known)				
Children of victim or perpetrator (under 18s only)				
V/S Pregnant – Yes/ No?				
Names of children (under 18)	**Date of Birth**	**Perp or Victim's child**	**Address -** if diff. to victim/perpetrator	**School** If known
BASIS OF REFERRAL & RELEVANT RISK FACTORS				
Include the date of the recent disclosure or incident that led to the referral to the Community Risk MARAC; *Details of support offered and/or taken up by the victim*				
Is the victim aware of Community Risk MARAC Referral? (Yes/No) If No, please state why:				
Referrer's name & organisation				
Telephone / Email				

Date referred to Community Risk MARAC	