INFORMATION SHARING AGREEMENT

INFORMATION SHARING AGREEMENT (ISA)

BETWEEN

Respect / Women's Aid Federation England

AND

DELIVERY PARTNER

Version - 1.0

SUMMARY SHEET

Information Sharing Agreement

Ref:	Make a Change

PURPOSE	To create a system for the formal exchange of information between all named parties to this agreement, with the intention to deliver Make a Change.

PARTNERS	DELIVERY PARTNER	
	Respect	The Green House, 244-254 Cambridge Heath Road, London E2 9DA
	Woman's Aid	Woman's Aid Federation of England, PO Box 3245, Bristol, BS2 2EH.
	This Information Sharing Agreement is a live document and will be updated and amended to include relevant Partner Agencies as they join, or leave, the partnership. Further signatories will be added after agreeing to the terms and conditions of this agreement and signing Appendix 4.	

Date Agreement comes into force:	To be confirmed

Date of Agreement Review:	Six months after coming into force, then annually. The agreement will be reviewed through the programme board.

Agreement Owner:	Respect and Women's Aid

Agreement drawn up by:	Victoria Cousins, Director of Make a Change

Location of Signed Agreement	Electronic

Protective Marking:	No protective marking

VERSION RECORD

Version No.	Date	Amendments Made	Authorisation
001	28 08 18	Initial Draft	
002	29 05 20	Reviewed for roll out	

1. INTRODUCTION

1.1 Respect and Women's Aid are committed to partnership working, and continually look for opportunities to work more closely with identified partners to identify, prevent and reduce domestic abuse.

1.2 In adopting this partnership approach it is important that the policies/practices of the agencies involved complement each other to ensure that any action taken is appropriate, necessary, proportionate, protects the dignity and privacy of adult and child victim/survivors and consistently applied.

1.3 This agreement outlines the need for the named organisations to work together in order to deliver Make a Change

2. PURPOSE

2.1 Make a Change has been developed by Respect, in partnership with Women's Aid Federation of England (WAFE), to deliver an early response to perpetrators of domestic abuse. Inspired by the Women's Aid Change That Lasts approach, and delivered by locally based organisations, we aim to create opportunities for change for those who use abusive behaviours in their intimate relationships.

Those who work with us are encouraged to Make a Change for:

Their community

Their organisation

Themselves

Make a Change recognises the complexity and variety of the causes of domestic abuse perpetration. We understand the importance of working with the cause of the problem to build lasting change for families and communities. We take a two-stage approach to delivery by raising awareness of the issue and then breaking down the barriers that communities, professionals and those who use abuse face in seeking and accessing support. The needs and safety of survivors are at the heart of our intervention.

2.2 A key factor for developing Information Sharing Agreements is to ensure that personal information is being processed fairly and lawfully. Identifying the ***Data Controller*** for personal information disclosed within the remit of this ISA will help determine the roles and responsibilities of each organisation. This should ensure that information sharing is both fair

and lawful. The recipient organisation will become the ***Data Controller*** for any personal information that is shared for the purpose/s described within this ISA.

3. POWER(S)

This agreement may fulfil the requirements of the following:

3. 1 Lawful basis for information sharing under the DPA and/or the GDPR

- The sharing of information in relation to this agreement is lawful as it meets:

➢ Article 6 (1) (a) Consent – The data subject had given consent to the processing for one or more specific purposes.

If a situation arises where a legal obligation exists, then Article 6 (1) (c) will be met: Legal obligation – Processing is necessary for compliance with a legal obligation.

If a situation arises whereby information needs to be disclosed to protect the vital interests of an individual, then Article 6(1) (d) will be met:

Vital Interest – Processing is necessary in order to protect the vital interests of the data subject or another person.

➢ Article 9 (2) (a) Consent – The data subject has given explicit consent to the processing for one or more specific purposes.

Article 9 (2) (d), (f) and (g) may be met in relation to information sharing through the Make a Change

Disclosures which are not based on explicit consent will be accessed on a case-by-case basis to ensure that any information shared under this agreement is lawful and a condition for processing is met.

3.2 Legislation which requires consideration prior to the disclosure of information:

- The Civil Evidence Act 1995;
- The Crime and Disorder Act 1998 (section 115);
- Common Law Powers of Disclosure;
- The Rehabilitation of Offenders Act 1974;
- The Human Rights Act 1998 (article 8);
- The Data Protection Act 2018 (Schedule 2, Part 1 (2) & Part 1 (5) (1-2) & Schedule 8 Part 3 & 4);
- General Data Protection Regulation (GDPR) (EU) 2016/679
- The Children Act 1989 (amended under the Adoption of Children Act 2002)
- Working Together
- Safeguarding Adults: A National Framework of Standards for good practice and outcomes in adult protection work (ADSS 2005)

4. CONSTRAINTS ON THE USE OF INFORMATION

4.1 This agreement has been formulated to facilitate the exchange of information between partners. However, it is incumbent on all partners to recognise that any information shared must be justified on the merits of each case.

4.2 The sharing of personal data requires careful judgement in which the identified policing need must be considered against relevant issues dictated under Data Protection and Human Rights legislation. Any information the police or partner agency considers sharing must therefore be accurate, necessary and proportionate.

Accurate: All information must be accurate and relevant to the purpose for which it is being shared with proper reference made to the nature of the source and the information itself.

Necessary: The necessity to share information between the named organisation is to effectively deal with issues concerning the prevention, detection, investigation and prosecution of those persons engaged in criminal activity and/or anti social behaviour, and an ongoing responsibility to protect public safety.

Or The necessity to share information between the named organisation is to provide information for risk assessment purposes to ensure effective safeguarding strategies are adopted either on an individual or community basis.

Proportionate: In considering whether to share personal information all parties have a duty to ensure that a fair balance is achieved between the protection of an individuals rights and the general interests of society. In judging whether it is appropriate to share such information the named organisations will examine whether the identified purpose infringes upon the subject's right to privacy, the appropriate measures to meet the purpose are both fair and rational and also that the means used are no more than is necessary to accomplish the purpose.

4.3 Information Exchange

Information Exchange relates to a physical exchange of data between one or more individuals or agencies. Advice from the Information Commissioner indicates that public authorities may exchange data, provided that:

- They have notified their intention to do so
- That the process of exchange is in accordance with the Data Protection Act (DPA)/ the GDPR, in particular the six principles listed in section 35 – Section 40 of the DPA 2018 and Article 5(1) of the GDPR (See Appendix 1 for further information).
- There is a statutory or common law power to do so.

4.4 Fair Processing.

The Data Protection Act requires the fair processing of information unless an exemption applies. In particular, fairness involves being open with people about how their information is used. Lincolnshire Police have a privacy notice available on the website which states how the information may be processed and shared. Additionally, information sharing agreements are published on the Lincolnshire Police website.

4.5 Disclosure to third parties

If an agency wishes to disclose shared information to a third party, as best practice the agency should seek written consent from the agency that provided the information. If a statutory requirement for disclosure exists then consent for further disclosure is not required. Any agency must ensure that all principles of the Data Protection Act are adhered to. Therefore, if an agency makes a further disclosure to a third party they must ensure that the

sharing of personal data is not processed in any manner incompatible with the purpose/s it was obtained for.

4.6 As best practise all information shared is only valid at the time of provision, and should only be used for the purpose as requested. However, the recipient organisation becomes the ***Data Controller*** for the shared information therefore the information may be used for subsequent investigations, if it is being used for a purpose that is compatible with the purpose for which it was obtained for example for the prevention and detection of crime and disorder.

4.7 <u>Disclosures</u>

Disclosures of information and in particular, personal data are bound to both common and statute law in particular, but not restricted to the following:

- The Common Law Duty of Confidentiality
- The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) (EU) 2016/679
- The Human Rights Act 1998

Any disclosure of personal data must have regard to both common and statute law. For example, defamation, the common law duty of confidence and the data protection principles. Consideration should always be given to alternative powers that exist for the purposes of data disclosure:

4.8 Survivors, <u>Witnesses, Victims, Complainants and Children</u>

Extreme care and careful consideration should be taken where the disclosure of information includes details of survivors, witnesses, victims, complainants and children. The general rule is that information such as described by survivors, witnesses, victims, complainants or children should not be disclosed without consent. However, in cases where there is a significant safeguarding concern or pressing social need, best efforts will be made to obtain full informed, specific and explicit consent from the individual concerned. In all such cases, advice should be sought from the organisational Safeguarding Lead.

5. TYPES OF INFORMATION TO BE SHARED

5.1 Through the project governance framework a range of data and documentation will be shared by all parties signed under this agreement. This includes:

<u>Non- personalised data:</u>

- Anonymised performance information
- Anonymised participant feedback
- Research findings / reports
- Project Plan
- JDPS/Role profiles
- Financial reports
- Home Office Grant Agreement returns

5.2 **<u>Personalised data:</u>**

As the project develops there is an expectation that personal data will be shared amongst Partner Agencies. The disclosure of personal data will be reviewed at the Project Working Group as the project progresses.

The personal data which may be disclosed will include the following information:

- Personal details related to those using abuse to enable multi-agency checks as art of ongoing case management
- Case related Personal data such as tracking outcomes.
- Through the provision of quality assurance for example: Practice Advisors attending case management and reviewing treatment management

This is not an exhaustive list and will be amended as required in accordance with the needs of the project.

Disclosures will contain factual information only, using the principle that **'the minimum disclosure required is the maximum disclosure permitted'**. Should safeguarding concerns arise it is the responsibility of each organisation to adhere to its safeguarding policy and any disagreements should be managed through formal escalation processes as outlined, or in conjunction with, the Safeguarding Policy.

Convictions and cautions should not be disclosed if they are considered spent under the Rehabilitation of Offenders Act 1974. See Appendix 3 for further information on spent convictions.

6. ROLES AND RESPONSIBILITIES UNDER THIS AGREEMENT

6.1 Each partner should appoint a single point of contact (SPoC). The sharing of information must only take place where it is valid and legally justified.

Respect SPoC	Title: Respect National Head of Delivery and Development for Make a Change Contact details: 07543221082
WAFE SPoC	Title: Business Development Lead Contact details: 07825767533
Delivery Partner SPoC	Title: Contact details:

6.2 <u>Information Breaches</u>

Complaints and breaches to this agreement should be dealt with by utilising any established agency policies and procedures for breaches and complaints made in relation to appropriate

legislation in connection with the agreed information exchange and data processing. In the case of any data breach the Respect National Head of Delivery and Development for Make a Change must be informed within 24 hours

Any disclosure of information by an employee, which is done in bad faith or for motives for personal gain, will be the subject of an investigation and be treated as a serious matter. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents.

All agencies are reminded of the Data Protection Act/ GDPR Principles and Part 6, Section 170 (unlawful obtaining) and Part 7, Section 198 (liability of directors) Offences of the DPA 2018

It is the responsibility of all parties to notify the other party of any known breach or infringement immediately and remedial action must be agreed and actioned by all relevant agencies concerned.

Major breaches may result in this agreement being temporarily suspended or withdrawn completely.

6.3 Subject Access

Subject Access is an individual's right to have a copy of information relating to them which is processed by an organisation.

Once information is disclosed from one agency to another, the recipient organisation becomes the **Data Controller** for that information. With regards to subject access requests, the **Data Controller** has a statutory duty to comply with Part 3, Chapter 3, section 45 of the DPA (Article 15 GDPR), unless an exemption applies. It is good practice for the recipient organisation to contact the originating organisation. This enables the originating organisation to advise the use of any statutory exemptions that may need to be applied prior to disclosure to the requesting individual. Communication should take place speedily thus allowing the servicing of the request to take place within the Statutory 1 calendar month time period.

6.4 Right to erasure or restriction of processing

Under Article 17 of the GDPR, individuals have the right to request to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

If a party to this agreement has disclosed the personal data to others, they must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, they must also inform the individuals about these recipients.

Women's Aid contact details in relation to right to erasure requests: Lauren Owen

Respect: National Head of Delivery and Development for Make a Change

Delivery Partner: TBC

The notification should be made in writing and contain the following details :

- The date the information was disclosed;
- who the information was disclosed to and by whom (including contact details);

- a reference number if applicable.

Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

If a party to this agreement has disclosed the personal data in question to others, they must contact each recipient and inform them of the restriction of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, they must also inform the individual about these recipients.

The Notification process is as described above for requests for erasure.

6.5 **Disagreements and conflict**

Each delivery partner is responsible for adhering to their own safeguarding policy. Where there is disagreement as to the actions of the party and these should be sought to be resolved locally between service managers. Where this is not possible, the Respect National Head of Delivery and Development for Make a Change and Women's Aid Business Development Manager should be consulted for advice. Should a resolution be impossible at this point, the issue must be escalated to the Project Board (lead by Respect and Women's Aid). If this is urgent, this can be managed out of the normal meetings of the board, and the Respect National Head of Delivery and Development for Make a Change and Women's Aid Business Development Manager will facilitate this.

6.6 Escalation

When referring to other agencies any safeguarding concern or issue that cannot be resolved though referral and follow up, the delivery partner must notify the Respect National Head of Delivery and Development for Make a Change

The Respect National Head of Delivery and Development for Make a Change must be informed of any incidents, accidents or issues that that are critical in nature

All notifications must be made within 24 hours.

7. SECURITY

7.1 Partner agencies should establish common rules for shared data security, in order to ensure compliance with the Data Protection Act. As best practice the disclosing organisation should make sure that any personal information they disclose will continue to be protected by ensuring that the recipient organisation has adequate security measures in place. Laptops must be encrypted. It is the responsibility of all delivery partners to work with the partnership to proactively address logistical challenges in sharing information.

7.2 As part of Respect/WAFE's responsibility regarding the data they process/control, the security guidance within this document should be agreed to and signed up to by all the parties involved within this agreement. However, it must be noted that the recipient agency/ies has legal responsibility for any information that has been shared as a result of this information sharing agreement, this includes its security.

7.3 Agencies that have adequate security measures in place to ensure compliance with the Data Protection Act should apply their own security procedures to any shared information.

7.4 Respect and WAFE may, by arrangement undertake a physical review of a partner agency's premises and security procedures.

7.5 Security Guidance

It is essential that the participating agencies provide personal or other sensitive information only to specific individuals authorised to receive it. The transfer, use, storage and retention of the information by each participating agency must comply with the Data Protection Act, and should comply with the security requirements stipulated within this agreement. Any additional security requirements that an agency wishes to specify must be done so in agreement with all parties involved within this document.

7.6 General Principles

Ensuring that personal information is protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access is the sixth principle of the Data Protection Act 2018. Partners should ensure they have appropriate security in place and arrangements to monitor these.

A key issue, especially for electronic documentation, is the consistent use of encryption and secure information exchange. Unguarded exchange of personal information may not only infringe the rights of the individual subject or others that may be identifiable from the information, but also compromise the organisations sharing information or jeopardise any proceedings or legal measure based upon that information.

With remote working there is an issue about storing personalised information on flash drives/memory sticks and of encryption. Partners sharing personal information are responsible for ensuring laptops, drive or removable electronic media containing personal information used for remote working are encrypted. Recent Home Office guidance with respect to third party suppliers suggests that:

a) No unencrypted laptops or drives or removable electronic media containing personal information should be taken outside office premises.

b) No transferring of any protected personal information from Home Office approved systems to third party suppliers owned laptops, PCs, USB keys, external drives and any other electronic media is permitted.

7.7 Secure Information Exchange

Electronic exchange can be the most secure and auditable means of exchanging information provided this is done using suitable secure technology. Personal information should only be exchanged electronically using a secure messaging system.

Attendees at meetings where personal data is discussed must also ensure that controls applied to agenda and minute documents as are as secure as those used for requesting and securing personal information, since these will often name the individuals being considered and contain elements of the information contributory to the decision making process. Records of meetings and personal information must be subject to the principles set out in the ISA, particularly in relation to purpose and retention.

If a recipient organisation wishes to remove shared information from their premises, they must ensure that the information is kept secure at all times, must not be made available to individuals who are not authorised to see it, and must only be used for the purposes specified within the 'Information Sharing Agreement'

7.8 Sharing information securely

It is important that information is shared securely. Those who receive personal data should take appropriate measures to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing. This includes when data is being shared and stored both electronically and manually (e.g. paper).

All designated Officers who have access to personal data should have been assessed for reliability in line with the employer's requirements for the role, for example Disclosure and Barring Scheme (DBS) checks. A greater degree of staff vetting and/or training is needed where there is a greater importance that relevant data be secure.

The information Commissioner has issued the following guidelines concerning obligations for agencies:

a) Does the data controller have a security policy setting out management commitment to information security within the organisation?

b) Is the responsibility for the organisations security policy clearly placed on a particular person or department?

c) Are sufficient resources and facilities made availability to enable that responsibility to be fulfilled?

Shared information should be stored securely, and if no statutory guidance dictates otherwise the recipient organisation should destroy the information when it is no longer needed for the purpose for which it was provided. If an organisation does not have the means to securely destroy shared information, they should consider returning the data to the originating organisation for destruction.

7.9 Transmitting information securely

When sharing information both the sender and the receiver should deal with the information according to its protective marking. See Appendix 2 for handling requirements in line with information classification.

Any e-mail or attachment containing personal data must be sent via a secure encrypted e-mail system. Where the partner does not have access to a secure encrypted e-mail system, the information must be encrypted via some other means, such as Windows password encryption, and the password sent via other means, such as telephone.

8. INFORMATION SHARING PROCESS

8.1 Information will be shared using the following methods:

- **Secure email:**

  Relevant project information will be disclosed via secure electronic means on a monthly basis.

8.2 Information sharing may be shared on an ad hoc basis when necessary. Ad hoc information should be shared using the following procedure:

Handling Requests for ad hoc Information - requests for information from the project will be handled and logged on the project plan master document held by the partners. Decisions regarding responses will also be recorded.

9. REVIEW, RETENTION AND DELETION

9.1 The recipient of the information is required to keep it securely stored and when it is no longer required for the purpose for which it was requested, will safely dispose of it. In order to ensure compliance with the Data Protection Act, data should be kept no longer than is necessary, retention periods may vary between organisations. Respect and WAFE and the named delivery partner will retain copies of the requests and responses for 6 years.

Partner agencies should retain the shared information in accordance with statutory guidelines and internal policies. If no statutory guidance exists for the retention and deletion of data, information should be held in accordance with the fourth (d) and fifth principle (e) of the DPA/ GDPR.

9.2 Files containing information from partner sources will be reviewed in line with policy.

10. REVIEW OF THE INFORMATION SHARING AGREEMENT

10.1 This Information Sharing Agreement will be reviewed six months after its implementation and annually thereafter. The nominated holder of this agreement is Respect. It is based on the national template for Information Sharing which forms part of the guidance issued on the Management of Police Information by the National Police Chiefs' Council (NPCC) the Home Office.

11. INDEMNITY

11.1 Recipient organisations will accept liability for a breach of this Information Sharing Agreement should legal proceedings be served in relation to any, failure, breach or default involving the received information. The recipient organisation cannot be held liable if a breach occurs that is attributable solely to any failure, breach or default on the part of the Information Provider.

11.2 The data recipient shall indemnify the Information Provider in full in respect of any loss or damage caused to the Information Provider as a consequence of the unauthorised disclosure of data supplied under this agreement.

12. DISCLAIMER

12.1 The Information Provider disclaims all liability to the data recipient in connection with the data recipient's use of data supplied under this agreement and shall not, under any circumstances, be responsible for any special, indirect or consequential loss or damages including but not limited to loss of profits arising from the use of the data by the data recipient.

13. SIGNATURE

13.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purposes of this agreement.

13.2 Signatories must also ensure that they comply with all relevant legislation.

13.3 It is the responsibility of all signatories to ensure that:

- Realistic expectations prevail from the outset.
- Professional, ethical standards are maintained.
- The Data Protection Principles are upheld.
- The information exchanged is kept secure and confidentiality is maintained as appropriate to the information's level of protective marking as defined by the Data Controller.
- A mechanism exists by which the flow of information can be controlled.
- Appropriate staff training is provided on this agreement.

13.4 Adequate arrangements exist to test adherence to the agreement.

Signed on behalf of Respect .....

Name: .....

Position: .....

Date: .....

.....

Signed on behalf of WAFE .....

Name: .....

Position: .....

Date: .....

Signed on behalf of Delivery Partner .....

Name: .....

Position: .....

Date: .....

Appendix 1

Appendix 1– Principles of the Data Protection Act (Part 3 Chapter 2 Section 35 – 40) / General Data Protection Regulations (Article 5 (1))

Principle 1 (a)	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
Principle 2 (b)	Personal data shall collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
Principle 3 (c)	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
Principle 4 (d)	Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
Principle 5 (e)	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
Principle 6 (f)	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Appendix 2

ADDITIONAL SIGNATORIES TO THIS AGREEMENT

I, the undersigned, on behalf of my organisation, agree to the terms of this Information Sharing Agreement.

Signed on behalf of .....

Title: .....

Position: .....

Date: .....

Please retain a copy and send the original to: Respect, 4th Floor, Development House, 56-64 Leonard Street, London , EC2A 4LT