Ending domestic abuse

Marac Information Sharing Protocol Checklist

The following checklist sets out the key contents of a Marac Information Sharing Protocol (ISP); it is designed to act as a guide to help you draw up your own protocol locally and does not constitute legal advice. The headings listed below provide the basic structure for a generic ISP. There may be additional information that you feel is relevant to your area and that you would like to include. You must check your ISP with your own, local legal advisors.

Understanding issues around sharing information without consent are crucial when writing an ISP. Some of those issues are addressed in the frequently asked questions on disclosure of information before and during the Marac meeting document, available from SafeLives. You are also advised to contact the Information Commissioner's Office for guidance on specific issues relating to information sharing.

I. Introduction

- Outline the purpose of the Marac Information Sharing Protocol.
  - *Example: The purpose of the* Marac *Information Sharing Protocol is to set out the legal grounds for information sharing between all agencies who have agreed to work together within the* Marac *framework in accordance with the relevant legislation (including The Data Protection Act (1998), The Children Act (1989 and 2004), Human Rights Act (2000) and any other relevant legislation as listed below) in order to: increase the safety of all victims, including children; enable the protection of vulnerable people; and reduce crime and disorder locally.*
- List all relevant legislation.
  - *Example: The Data Protection Act (1998), The Children Act (1989 and 2004) and The Human Rights Act (2000) etc.*
- Explain how the protocol sits with other inter-agency information sharing agreements in operation.
  - *Example: The* Marac *Information Sharing Protocol is designed to enhance existing arrangements rather than replace them.*
- List all signatory agencies.
- Set out the commitments of signatory agencies.
  - *Example: To share information in high risk situations, to comply with all relevant legislation, to register with the Information Commissioner's Office, to seek their own legal advice, to use the data disclosed only for the agreed purpose etc.*

II. Data

- Specify the nature of the data each agency will share regarding victim, child(ren), perpetrator(s) and possible future partners.
  - *Example: Police will share crime incidents, offender information etc.; housing will share vandalism records, neighbourhood complaints etc.*

- Define the different types of data to be shared (non-personal data, depersonalized data, personal data and sensitive personal data) and outline the different ways in which these types of data will be used.

- Outline the statutory gateways for information sharing.
  - *Example: Explain how the relevant provisions of the Crime and Disorder, Human Rights, and Data Protection Acts allow for information sharing in certain circumstances.*

- Explain best practice around obtaining consent from the victim.
  - *Example: It is best practice to obtain consent but not obligatory in high risk cases and this approach is not always safe.*

- Outline where public interest overrides the need to obtain consent from the victim.

- Highlight the need for proportionality to govern decisions made about sharing information.
  - *Example: Signatory agencies should consider the perpetrator's right to a private life under Article 8 of the Human Rights Act, and balance this with the need to share information.*

- Set out the role of the data controller/ single point of contact for each signatory agency.
  - *Example: The data controller must be of a sufficient standing within the signatory agency to have a coordinating and authorising role as they are responsible for ensuring that the agency they represent obeys the protocol and all relevant legislation, etc.*

III. Process

- Outline how signatory agencies meet disclosure requests.
- Outline how signatory agencies meet subject access requests (e.g. by the victim or perpetrator).
- Explain how signatory agencies will agree on the criteria for 'weeding' data.
- Specify the key principles when handling media involvement in relevant cases.
- Information sharing with and referral to and from other Maracs.
  - *Example: Consistency, honesty, impartiality, and a consent-based approach when making information public.*

IV. Security and data management

- Set out an acceptable standard of security when storing and processing data so that its integrity and confidentiality are maintained at all times.
- Outline how use of information outside of the meeting is governed. Outline how long data should be kept after it is first collected.

V. Complaints

- Outline the process for making a complaint against another signatory agency about their Marac activities or processes.

VI. Breaches

- Highlight that a breach of this protocol would be extremely damaging for all signatory agencies.

VII. Review

- Specify a date for reviewing the Marac Information Sharing Protocol.

VIII. Withdrawal

- Make clear the process for and implications of withdrawing from the Marac Information Sharing Protocol.

IX. Signatories

- Provide space for agencies attending the Marac to sign the Marac Information Sharing Protocol, specifying their name, the agency they represent, and the date of signature.

Suggested appendices

You could also consider attaching the following to your Marac Information Sharing Protocol:

- The recommended SafeLives Dash Risk Identification Checklist (Ric) for Marac agencies
- Marac Referral Form
- Marac Research Form
- An Information Sharing Without Consent Form