East Lothian and Midlothian Public Protection Committee

Marac Information Sharing Protocol

Version 1 approved at EMPPC on 19 September 2023

Contents

Part A – Introduction to this Information Sharing Protocol (ISP)

1. Scope and purpose

The purpose of this ISP is to support the regular sharing of personal information in dealing with high risk cases of domestic abuse through the Multi Agency Risk Assessment Conference (Marac) process.

The document details the specific purposes for sharing and the personal information being shared, the required operational procedures, consent processes, and lawful justification.

Proportionate and relevant information sharing is the key to a successful Marac in order to facilitate effective safety planning while protecting the rights of the individual.

The Marac process identifies high risk victims of domestic abuse and aims to reduce the risk of further victimisation through:

- Appropriate sharing of information across agencies;
- Producing multi-agency safety plans to reduce the risk to victims and any children and;
- Sharing an awareness of risk posed by the perpetrator to the victim or third party.

The ISP covers the exchange of information between all partners involved in the Marac process in East Lothian and Midlothian. The coordination of the Marac Process is undertaken by the Marac Coordinator, who is located within the East Lothian and Midlothian Public Protection Office (EMPPO). This is an administrative shared service between the two local authorities, not a legal entity.

This information may also be shared to support the effective administration, audit, monitoring, inspection of services and reporting requirements. Partners may only use the information disclosed to them under this ISP for the specific purpose(s) set out in this document.

2. Definitions

Criminal Offence Data - personal data relating to criminal convictions and offences or related security measures.' It covers a wide range of information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings. It may also include personal data about unproven allegations and information relating to the absence of convictions.

Data Breach – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Data controller – the body that decides how the data will be processed. For the purposes of this ISP each partner organisation is considered a separate data controller. For the avoidance of doubt, the EMPPO is not a Data Controller.

Data Incident – A generalised term referring to a data breach, near miss, or other event relating to or causing an increase in risk to privacy.

Data Protection Legislation – the Data Protection Act 2018 ('DPA2018'), the UK General Data Protection Regulation ('UK GDPR') and any successor legislation as added and amended from time to time.

Data Subject – the individual identified directly or indirectly by the personal data and to whom the personal data relates.

Partner organisations – all organisations represented at East Lothian and Midlothian Marac.

Personal Data – as defined in the Data Protection Legislation. For the avoidance of doubt, any information relating to an identified or identifiable individual.

PCR – Person Causing Risk.

Service user – this will refer to victim, perpetrator and any related child discussed at Marac.

Special Category Data – personal data relating to race, ethnic origin, political opinions, religious/philosophical belief, trade union membership, genetic data, biometric data, health data, or data concerning sex life/sexual orientation.

3. Functions

Marac partners will share information to support the Marac aims:

- Work with victims of domestic abuse to help keep them safer and respond to their needs;
- Manage perpetrators' behaviour to reduce risk;
- Ensure that risk and support needs attached to family members or extended networks are identified;
- Maintain the safety and welfare of professionals and
- Make links with other protection processes (such as Child Protection, Adult Support and Protection, Multi-Agency Task and Coordination groups, Multi-Agency Public Protection Arrangements).

Personal information shared to support functions other than those detailed above are not supported by this ISP.

4. Principles of Sharing Information

Staff should not hesitate to share personal information in order to prevent abuse or significant harm, in an emergency situation. **Adult Support and Protection Procedures** and **Child Protection Procedures** must be followed if there are such concerns.

Article 5 of the GDPR sets out seven key principles which lie at the heart of general data protection.

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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; ('storage limitation');

(f) 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')."

(g) Article 5(2) adds that: Data controllers are responsible for and must be able to demonstrate compliance with Data Protection principles.

5. Service Users included

The ISP relates to high risk cases of domestic abuse (usually aged 16 and over).

Information will also be shared in relation to:

- Victim(s);
- Perpetrator(s);
- Any child at risk under the age of 18 (in line with UNCRC); and
- Any other person deemed to be at risk, is a protective factor, or posing a risk in relation to the case.

6. Details of personal information being shared

Only information that is necessary and proportionate to the purposes should be shared.

Information below may relate to the service users noted above.

The information shared may include:

- Name, date of birth, address(es), aliases and gender;
- Current information relating to recent contact, meetings, sightings, phone calls between any of the service users and any of the partner organisations. This could include attendance or non-attendance at appointments and who is present at an address;
- Current information on attitude, demeanour, behaviour, etc. This may include professional judgement relating to these elements and/or information from the victim about them;
- Information about court orders, injunctions, bail conditions and other legal issues;
- Historic information such as, previous convictions, family relationships history, other safety options considered, substance misuse issues, mental health concerns; and
- Other information relating to the risks facing the victim or other individuals potentially affected by domestic abuse.

7. Key identifying information

When sharing information, the following identifiers will be used where available, to accurately identify Data Subjects and to ensure that all partner organisations are referring to the same Service User (victim, perpetrator or child):

- First Name
- Surname
- Aliases
- Address
- Date of birth

8. The information sharing partner organisations

This ISP covers the exchange of information between staff of the following organisations. For the purposes of this ISP each partner organisation is considered a separate Data Controller.

East Lothian	Midlothian
Police Scotland	Police Scotland
Women's Aid East and Midlothian	Women's Aid East and Midlothian

Edinburgh Women's Aid	Edinburgh Women's Aid
Shakti Women's Aid	Shakti Women's Aid
SACRO	SACRO
East Lothian Council	Midlothian Council
NHS Lothian	NHS Lothian
Scottish Fire and Rescue Service	Scottish Fire and Rescue Service

Staff of the partner organisations listed above who engage in Marac data sharing are expected to familiarise themselves with this Protocol and abide by its terms.

The term 'staff' encompasses paid workers, volunteers, students and other temporary workers approved by the employing / hosting organisation, whose duties include those relating to the functions outlined in this ISP.

Partner organisations will ensure that Marac Representatives and all other relevant staff, receive appropriate training in the application of this ISP and relevant legislation.

Information discussed and shared by the partner organisations in relation to the Service Users as part of the Marac process is strictly confidential and must not be disclosed to third parties who have not signed up to this ISP.

Occasionally organisations which are not signed up to the ISP may be invited to Marac if they have relevant involvement in a case. In these circumstances they will be asked to sign a confidentiality form prior to attending the meeting.

Part B – Justification for sharing personal information

9. Legislative framework

As separate Data Controllers, each Partner Organisation is responsible for independently determining the appropriate lawful basis for its processing of personal data. The following sets out the legal gateways that are most likely to apply to the data sharing under this Protocol.

The lawful bases for information sharing are contained within Articles 6, 9 and 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018. The processing of all personal data must meet a condition under Article 6 to be lawful; the processing of Special Category and Criminal Offence Data must also meet additional conditions under Articles 9 or 10 and Schedule 1.

For the purposes of processing Special Category and Criminal Offence Data, the Partner Organisations should hold an appropriate policy document which outlines their compliance measures and retention policies.

For further information on GDPR see the Information Commissioner's Office Guide to the UK General Data Protection Regulation (UK GDPR).

9.1 Article 6 conditions – Personal Data

9.1.1 Vital Interests - Article 6(1)(d) of the UK GDPR states that "processing is necessary in order to protect the vital interests of the data subject or of another natural person". Vital Interests can be used by all partner organisations where there is an immediate risk to life.

9.1.2 Public Task – Article 6(1)(e) of the UK GDPR states that "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". Public Task should be used by public authorities where the risk to life is not immediate.

9.1.3 Legitimate Interests – Article 6(1)(f) of the UK GDPR states that "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child". Legitimate interests should be used by non-statutory Partner Organisations; it should not be used by public authorities when another lawful basis applies. When used, a Legitimate Interests Assessment should be carried out by the organisation that is sharing information.

9.2 Article 9 / Schedule 1 conditions – Special Category Data

9.2.1 Vital Interests – Article 9(2)(c) of the UK GDPR states that "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. This is more specific than the Article 6 condition for processing personal data such as names/addresses/identifiers, and may be used by all Partner Organisations where appropriate.

9.2.2 Substantial Public Interest – Article 9(2)(g) of the UK GDPR. Processing under this condition must also meet a Schedule 1 condition. The relevant conditions to this Protocol are:

Statutory and government purposes.[1] This condition is available only to statutory and government Partner Organisations;

[1] Data Protection Act 2018, Schedule 1, Part 2, Section 6.

Preventing or detecting unlawful acts.[2] This condition is available to all Partner Organisations. This condition only applies if seeking consent would prejudice the purposes for processing.

Safeguarding of children and of individuals at risk.[3] This condition is available to all Partner Organisations. There are limitations on the use of this condition if consent can reasonably be obtained.

9.2.3 Explicit consent – Article 9(2)(a) of the UK GDPR. This condition is most likely to be relevant to non-statutory Partner Organisations if the Substantial Public Interest or Vital Interest conditions do not apply. This condition will not normally be the most relevant for statutory and government Partner Organisations.

9.3 Article 10 / Schedule 1 conditions - Criminal Offence Data

9.3.1 Any Partner Organisations who would rely on Substantial Public Interest for processing Special Category Data as set out above may also rely on these conditions to process Criminal Offence Data.

9.3.2 Police Scotland shall typically carry out processing of criminal offence data on the basis of official authority (Article 10(1) of the UK GDPR). In circumstances where official authority does not apply, Police Scotland may rely on another lawful basis, including the Substantial Public Interest conditions listed above.

10. Disclosure of information to third parties

Anyone not identified as a partner organisation in Section 8 is considered a third party. Disclosure needs to be determined by the individual circumstances of each case and who is making the request. There may be restrictions where information cannot be shared with 3rd parties. For further guidance refer to your Data Protection Officer.

Part C – Operational procedures for this ISP

11. Fair processing of information

Under Article 15 of GDPR, Data Subjects have a number of rights in relation to their information. These include:

- The right to be informed about how their information will be used.
- The right to access their personal information. Normally this is done by placing a 'Subject Access Request'. For more information on placing Subject Access Requests, please visit https://www.eastlothian.gov.uk/info/210598/access_to_information or

[2] Data Protection Act 2018, Schedule 1, Part 2, Section 10.
[3] Data Protection Act 2018, Schedule 1, Part 2, Section 18.

Request a copy of your information (DRAFT) | Subject Access Request | Midlothian Council.

- The right to ask to correct inaccurate or incomplete information.
- The right to have their personal information erased.
- The right to ask to limit the ways their information is shared or used.
- The right to ask for their information to be shared or moved to another organisation in an electronic format.
- The right to object to the ways their information is processed.

For further information please visit Individual rights | ICO

12. Information collection

The approved collection tools for partner organisations to gather and share the personal information detailed in this ISP are:

Risk Assessment Tools - Domestic Abuse, Stalking and Honour Based Violence Risk Identification Checklist (DASH RIC); Domestic Abuse Questionnaire (DAQ), or Spousal Assault Risk Assessment (SARA);

- Marac Referral form;
- Marac Agenda;
- Marac Research Form;
- Marac Action Log, and
- Marac Minute.

All information will be shared via secure e-mail.

13. Frequency of information sharing

The personal information outlined within section 6 will be only be shared on a need-to-know basis to support the functions of this ISP.

14. Retention Schedules

Personal data will be held, processed and then destroyed securely in accordance with the retention schedule and local policies and procedures of each partner organisation.

15. Information security

As each partner organisation is a separate Data Controller, any data breach involving information provided by another Party to the Protocol should be reported to the originating Party.

While joint consultation on taking a decision to report a data breach to the ICO or the Data Subjects will be encouraged, each Party has an independent obligation as a Data Controller

to assess the incident and take a decision whether the risk meets the 'likely risk' threshold for reporting to the ICO or the 'high risk' threshold for reporting to the Data Subject(s).

16. Records management

Each Party is responsible for storing and disposing of the shared data which they hold in line with their own Retention Schedule and disposal procedures. Staff carrying out functions outlined in this ISP should make themselves aware of their organisation's records management procedures.

Inaccurate, incomplete or out-of-date information can have detrimental effect on Service Users. If information is found to be inaccurate, each partner organisation will ensure that their records and systems are corrected accordingly. Consideration will also be given to advising partner organisations.

17. Complaints

Each partner organisation has a formal procedure by which Data Subjects can direct their complaints regarding the application of this ISP.

18. Review

This ISP will be reviewed every two years. Responsibility for reviewing this ISP will lie with the Marac Steering Group.

Author's name	Katerina Gradeva
Designation	Marac Coordinator
Date	01/08/2023
Next Review	01/08/2025