MARAC Information Sharing Agreement

Title of ISA: British Forces Germany Multi Agency Risk Assessment Conference Information Sharing Agreement

Purpose: For use by MARAC representatives

Date Agreement comes into force: Dec 15

Date of Agreement Review: Jul 17

Agreement Owner: BFG Safeguarding Board

Agreement Author: Domestic Abuse Champion, HQ BFG

Version Record

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Date amendments made</th>
<th>Authorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>9 Jan 17</td>
<td>Annual Review</td>
<td>DAC</td>
</tr>
<tr>
<td>19 Jul 17</td>
<td>Review</td>
<td>DAC</td>
</tr>
</tbody>
</table>


Summary

1. This Information Sharing Agreement (ISA) sets out the obligations for parties attending a Multi-Agency Risk Assessment Conference (MARAC):
   a. To share or disclose information about service users.
   b. To maintain confidentiality.
2. It does not impose new obligations, but reflects current regulations and legislation.
3. This agreement will be published on http://bfgnet.de/safeguarding/board.html.
4. This agreement is the protocol for ensuring confidentiality whilst permitting the appropriate transfer and sharing of information between agencies involved in the prevention, detection and reduction of crime and disorder in BFG.
5. This agreement shall commence from Dec 15, and signatories are invited to sign a copy of the agreement.

Organisations Covered by this Policy

6. This agreement has been developed to meet the information security and confidentiality requirements for sharing personal data (that is data which relates to a living individual who can be identified by that data and other information likely to be in the possession of the recipient) across organisations within BFG.
7. Organisations and individuals involved in sharing information include: HQ BFG; Service Police; British Forces Social Work Services; Victim Safety Workers; Probation; Army Welfare Service; Commanding Officers; Unit Welfare Officers; SSAFA / GSTT LLP (including Midwifery and Mental Health Services); DIO Housing; and Service Children’s Education (including British Forces
Early Years). It is recognised that organisational boundaries are changing and this policy can include any organisation (and any successor organisation) in any area that becomes a signatory to this policy.

Introduction

8. This ISA sets out the arrangements for sharing confidential information about particular individuals between the members of BFG MARAC’s.

9. It aims to encourage greater confidence in sharing information and, as a consequence, stimulate improved engagement between all parties involved in this initiative.

10. This agreement aims to clarify under which circumstances information will be provided by parties and later disclosed, in accordance with the MARAC process. The intention is that a single, multi-agency approach to share information is a highly efficient mechanism for reducing crime and disorder, including the protection of vulnerable persons and the community.

11. This ISA is an agreement between the signatories to share information about individuals for specified purposes. It has been developed to:
   a. Set out the purposes for which information needs to be shared.
   b. List the organisations which may share information under its terms.
   c. Identify the legal basis on which information can be shared.
   d. Describe the roles and structures that will support the exchange of information between parties.
   e. Ensure compliance with individual parties’ policies, legal duties and obligations.

12. The ISA should be read in conjunction with the BFG MARAC Operating Protocol and Guidelines.

Purpose and Scope of this Agreement

13. The purpose of this ISA is to ensure the MARAC:
   a. Provides a forum for multi-agency information sharing to improve the safety, health and well-being of victims and their children.
   b. Takes action and provides support that will reduce the risk of harm (physical or psychological) to victims of domestic abuse and their families.
   c. Determines whether an alleged perpetrator poses a significant risk to any particular individual or the general community.
   d. Reduces repeat victimisation.
   e. Improves agency accountability.

14. This agreement applies to the exchange and sharing of any information including computer held data, written exchange delivered by post/fax, email, and formal meetings between parties where minutes or notes are produced or actions recorded that support the aims listed above.

15. Information sharing at MARAC conferences is strictly limited to the aims of the meeting and attendees will sign a confidentiality declaration to that effect at the start of each conference. Information gained at the meeting cannot be used for other purposes without reference and permission from the person/agency that originally supplied it.

16. Home Office Guidance accompanying the Crime and Disorder Act 1998 states:

‘Effective information exchange is key to multi agency working in any sphere – nowhere more so than the statutory partnerships for Crime and Disorder reduction. It relies on good relations
between partners and above all on mutual trust. The effectiveness of information sharing arrangements is a reflection of the effectiveness of the partnerships as a whole.

Legislation and Guidelines

17. **Armed Forces Act 1991 - Part 3.** This enables orders to be made for the protection of the children of Service families, including children of civilian families subject to Service discipline. The Act does not detail express information sharing powers, but in practice it may be necessary to share information related to domestic abuse where it is relevant to the enable the exercising of powers under the Act.

18. **Human Rights Act 1998.** A disclosure to members of the same MARAC will comply with the HRA if it:
   a. Is made for the purposes of preventing crime, protecting the health and/or safety of alleged victims and/or the rights and freedoms of those who are victims of domestic violence and/or their children;
   b. Is necessary for the purposes referred to in (a) above and is no more extensive in scope than is necessary for the purposes; and
   c. Complies with all relevant provisions of law.

19. **Data Protection Act 1998.** The prevention of crime exemption under DPA can be used if disclosure to members of the same MARAC is necessary to prevent a crime against a named individual or specified household. The risk of crime must be credible.

20. **Criminal Prosecutions and Investigations Act 1996 (Application to the Armed Forces) Order 2009.** Where there is a current criminal prosecution, service police officers attending MARAC are obliged to inform the Service Prosecuting Authority of any evidence that might reasonably be considered capable of undermining the case for the prosecution against the accused or of assisting the case for the accused.

21. **Common Law Duty of Confidence.** An obligation of confidence will exist where the individual has provided the information to another in circumstances where it is reasonable to assume that the provider of the information expected it to be kept confidential. Where there is a duty of confidence the information can only be disclosed to third parties if one of the exceptions applies, namely if there is informed consent, compulsion by law, public interest or the information is in the public domain.

22. **Public Interest – Exception to the Duty of Confidence.** When considering whether to disclose information under this exception an individuals private right to confidentiality must be weighed against any relevant public interest factors in exchanging information and each case must be decided upon its merits. In determining whether the public interest would justify disclosure against the normal presumption of confidentiality, an objective assessment of all the available information must be made. Disclosure will engage Article 8 of the European Convention on Human Rights as incorporated into the Human Rights Act 1998. Public interest criteria will include:
   a. The prevention of crime and disorder.
   b. The reduction of crime and disorder.
   c. The detection of crime.
   d. Crime displacement.
   e. The apprehension of offender.
f. Reducing the fear of crime.
g. The protection of vulnerable members of the community.
h. Maintaining public safety.
i. The administration of justice.
j. Diverting young offenders.
k. National security.

23. **Proportionality of the Data Sharing.** The Human Rights Act 1998 incorporating the European Convention on Human Rights restricts public authorities in their use of private information. Article 8, the Right to Respect for Private and Family Life is the most commonly referred to article when considering and dealing with requests for disclosure of information. The right is qualified, in that it may be interfered with where this is in accordance with the law and is necessary in a democratic society:
   
a. In the interests of national security.
b. In the interests of public safety.
c. In the interests of the economic well being of the country.
d. For the prevention of disorder or crime.
e. For the protection of health or morals.
f. For the protection of the rights and freedoms of others.
g. When the human rights of any individual are considered to be actually or potentially engaged by a disclosure under the Agreement, the decision makers involved should ask themselves whether their actions are justifiable, appropriate, proportionate, auditable and necessary (JAPAN). To be proportionate the disclosure must only go as far as is necessary to achieve the desired aim.

24. **Vulnerable Adults Department of Health – No Secrets (2000).** The principles can be summarised as:
   
a. Information will only be shared on a need to know basis when it is in the best interests of the service user.
b. Confidentiality must not be confused with secrecy.
c. Informed consent should be obtained but, if this is not possible and other vulnerable adults are at risk, it may be necessary to override the requirement and

d. It is inappropriate for agencies to give assurance of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other vulnerable people may be at risk.

25. **Caldicott Guidelines on Information Sharing.** The Caldicott guidelines affirm the individual’s wishes should be respected unless there are exceptional circumstances. It is important to remember that these are guidelines and not law and that the Data Protection Act, the Human Rights Act and the common law duty of confidence will always take precedence. If there is an apparent conflict between legislation and the common law, the legislation must take precedence.

26. NHS and social care organisations must have procedures to control access to patient/person identifiable information. A Caldicott ‘Guardian’ should be appointed as gatekeeper of individual information. The Caldicott Guardian should agree who has access to what information. Caldicott Guardians can delegate their information sharing responsibilities, if they so wish, to someone else in their organisation. This person must be familiar with current legislation, guidance and best practice. Similarly, in relation to the Department of Health document “No Secrets” (2000) approach, it is inappropriate for agencies to give assurance of absolute confidentiality in cases
where there are concerns about abuse, particularly in those situations when other vulnerable people may be at risk.

27. Cases considered at MARAC are likely to constitute exceptional circumstances as defined in the Caldicott Guidelines because MARAC’s are forums to discuss the most serious cases of alleged or suspected domestic abuse but each case must be considered individually taking into account its specific circumstances.

28. **Management of Police Information (2005).** In addition it should be noted that the sharing of police information must meet one or more of the purposes set out in the statutory Code of Practice for the Management of Police Information (2005). The purposes are:
   a. Protecting life and property.
   b. Preserving order.
   c. Preventing the commission of offences.
   d. Bringing offenders to justice.
   e. Any duty or responsibility of the police arising from common or statute law.

29. **JSP 913 - Tri-Service Policy on Domestic Abuse and Sexual Violence.** This Tri-Service policy provides the framework for the MOD on how to deal with abuse and violence within the Armed Forces. It is to be used by all within the MOD as the basis for orders, instructions, procedures and training on domestic abuse and sexual violence that relates to all service personnel serving in the UK and overseas. This JSP also applies to all persons subject to Service Law and civilians subject to Service Discipline in certain overseas commands who are directly or indirectly involved in incidents of domestic abuse and sexual violence.

30. **JSP 770 - Tri-Service Operational and Non-Operational Welfare Policy.** This JSP provides the MOD’s welfare policy and guidance to Commanders at all levels as well as welfare specialists and unit budget managers on the provision of both operational and non-operational welfare to entitled personnel both at home and overseas.

31. **SI BF(G) 3341 - Information Sharing Protocol for British Forces Germany.** This protocol provides guidance to those in BFG working with children and young families. It gives guidance to practitioners who have to make decisions about sharing personal information with the ultimate aim of safeguarding and promoting the welfare of children and vulnerable adults.

**Sharing of Information**

32. Effective information exchange is the key to multi-agency working. It relies on good relations between parties, and above all on mutual trust.

33. **Personal Details.** The consent of a victim, informant, or a witness to the sharing of information should be obtained whenever possible. Care should be taken not to involuntarily identify other individuals whose consent has not been sought or obtained. If consent is not given, then agencies will need to decide on a case-by-case basis whether to share any information that they may have on the individuals. In principle, personal details of a victim, informant, or a witness should not be exchanged with another agency without the prior consent of the person concerned. This consent may be obtained either in writing or verbally, and in all cases must be recorded. In some circumstances the issue of consent can be addressed by clearly informing the subject that their details will be passed to the appropriate agency for action.

34. **Information Exchange without Consent.** It is acknowledged that it may be necessary to share information without consent when one of the lawful grounds for exchanging information are applicable and it is believed to be in the public interest.

35. **DASH.** The risk assessment (DASH) should be considered in all cases where the victim has not consented to information being shared, in deciding whether the threshold for disclosing
information without consent has been met. The referring agency should where appropriate, discuss their concerns with the victim and seek to obtain their consent to share information. If consent is still refused, the agency must then consider whether the circumstances justify sharing information without consent. If the decision to share the information is taken, then the referring agency must record that a decision has been made to share/disclose information without consent. The person providing that information should ordinarily be informed that it will be shared unless there are good reasons for not informing that person. The fact that she or he has been informed (or the reason for not informing her or him) must be recorded.

36. If the requirements for information sharing cannot be met, then the case cannot be referred to MARAC and the agency concerned is limited to providing intervention from its own resources. If the designated MARAC officer requires guidance on this issue, the advice of their legal department should be sought, and the chair of the MARAC may be consulted, but the decision whether to exercise discretion will always rest with the agency.

37. **Types of Information to be shared.** Personal information may be discussed at or subsequent to a MARAC meeting in respect of the alleged victim, any children or any of the parties involved in the alleged incident and the alleged perpetrator, and where relevant to the risks posed, the perpetrators family or other relationships. Information will not be shared by the parties receiving the information outside the meeting without the consent of the MARAC and the agency that originally supplied the information. Types of information that can be shared may be,

   a. Non-personal data which constitutes data that has never referred to individuals;
   b. De-personalised data which encompasses any information that does not and cannot be used to establish the identity of a living individual; and
   c. Personal data which is data that relates to a living individual who can be identified from those data, or from those data and other information, which is in possession of, or likely to come into the possession of, the data controller.
   d. Sensitive personal data is data that falls into the following categories; racial or ethnic origin, sexual preference, physical or mental health, membership of a trade union, political or religious beliefs and or criminal offences and proceedings.

38. The information discussed may cover the following areas:

   a. Name, date of birth, address(s), aliases and gender;
   b. Current information relating to recent contact, meetings, sightings, and phone calls. This could include attendance or non attendance at appointments, who is present at an address and attendance at emergency departments or other health settings e.g. mental health.
   c. Current information on attitude, demeanor, behaviour etc;
   d. Information about Court Orders, bail conditions and other legal issues;
   e. Historic relevant information such as previous convictions, family or relationship history, other safety options considered or alcohol/substance misuse issues;
   f. Issues relating to postings, deployments, absences, relevant conduct;
   g. Information regarding housing or accommodation options;
   h. Information regarding children’s attendance and behaviour at school;
   i. Other information relating to risks facing the victim or other data subjects.

39. Both personal and sensitive personal data must be clearly marked as personal data and kept securely within a pass-worded computer system or otherwise physically secure with appropriate levels of staff access. Partners must undertake to destroy all personal information when no longer required for the purpose in which it was intended.
The Information Sharing Process

40. **Single Point of Contact.** Each organisation/department/unit will appoint a single point of contact (SPOC) that will be an officer or manager of sufficient standing to have a coordinating and authorising role. SPOCs will appoint one or more designated officers to deputise when necessary and keep an updated list of designated officers for their agency. The SPOC will be:

   a. Expected to collate information from their organisation prior to the MARAC.
   b. Will represent their organisation at the MARAC meeting.
   c. Will ensure that their organisation has systems in place to identify victims of domestic abuse.
   d. Will record details of the persons being heard at MARAC, even where they have had no contact with their organisation. This will ensure that if they present to the organisation at a later date, the organisation will recognize that the person has been heard at MARAC previously.

41. **Record of Disclosure.** Initial disclosure will be recorded on the agenda circulated prior to the MARAC and then disclosure at the meeting will be recorded on the minutes.

42. **Onward Transmission of Personal Data.** The disclosing organisation retains ownership of the data that will only be used for the purpose specified. The recipient will not release the data to any third party without obtaining the express written authority of the disclosing organisation in advance.

43. **Security.** Organisations will ensure there is appropriate security for the safe and secure transportation or transmission of information. It is the individual agencies responsibility to ensure any information they note at the MARAC is secure. There is an absolute requirement for all agencies to hold information securely. It is the individual partner’s responsibility, as signatories to this agreement, to ensure that they have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information we hold. As a minimum, where kept electronically this must be on a pass-worded computer system within a secure folder. Parties with secure email should ensure all correspondence or documentation relating to MARAC is kept on a work based terminal only. Where hard copies are kept these must be stored in a locked cabinet within a secure office.

44. **Vetting.** It is the responsibility of the agency partner to ensure that their MARAC representative is appropriately vetted for this process. Agencies should have regard to their in house protocols in respect of retention and disposal. Appropriate technical and organisational measures shall be taken by partners against unauthorised or unlawful processing of information and against accidental loss or destruction of or damage to information.

45. **Accuracy of Information.** It is also the responsibility of each agency partner to ensure that information shared at MARAC or subsequent updates is accurate. Where an agency becomes aware that information shared by them is inaccurate or no longer relevant then they must inform the coordinator who will update the records held and notify relevant parties.

46. **Organisational Responsibility.** In signing this agreement, each signatory is undertaking to adopt the agreement on behalf of his or her organisation; appoint a SPOC and deputy who should receive information regarding MARAC cases, research agency files, consider whether disclosure is relevant on a case-by-case basis and attend the MARAC. Each organisation will ensure that:

   a. All staff are aware of the need for information security and confidentiality and to comply with this agreement.
   b. The SPOC is widely known within the organisation.

47. **Agreement.** Parties to this protocol accept that the procedures and processes identified in this document will provide a secure framework for the sharing of information between organisations
which will reduce the risk, related to incidents of domestic abuse. It does not create a contractual relationship nor is it intended to alter the legal relationships between the parties.

48. **Retention and disposal.** Partners will retain copies of minutes and any other notes for no longer than a period required by legislation or their own policy. Each partner will be responsible for the safeguarding of information. When the information is no longer regarded as being relevant, the partner will be responsible for its secure disposal/destruction. Information will be deleted if:

   a. The information has been shown to be inaccurate, in ways which cannot be dealt with by amending or appending the record.

   b. It is no longer considered that the information is necessary for police or the partners’ legitimate purposes.

   c. It reaches the end of the agreed retention period in each partner agency.

**Withdrawal**

49. Any partner may withdraw from this agreement upon giving written notice of three months to the other signatories. The partner must continue to comply with the terms of this agreement in respect of any information that they have obtained through being a signatory. Information, which is no longer relevant, should be returned or destroyed in an appropriate manner.

**Review**

50. This ISA will be reviewed annually by the DAC or sooner in the emergence of best practice. The review will:

   a. Ensure the contact list for MARAC representatives is up to date.

   b. Consider whether the agreement is still useful and fit for purpose.

   c. Identify any emerging issues.

   d. Determine whether the agreement should be extended for a further period (up to one year) or whether to terminate it.

**Complaints**

51. In accordance with JSP 831 Redress of Individual Grievance: Service Complaints, the intent is that complaints are dealt with at the lowest level possible and resolution is achieved quickly and where possible informally. Any complaints/breaches of this agreement, in the first instance, need to be raised with the Chair. If necessary the chair will refer to the agency’s internal complaints procedure.

52. Complaints and or breaches of the agreement may be discussed at the Domestic Abuse Forum and progressed to the Safeguarding Board as necessary. If the complaint requires the Policy to be reviewed, no action will be taken without the consent of all parties to this Policy.

**Signatories**

53. By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained and appropriately vetted so that requests for information and the process of sharing itself is sufficient to meet the purpose of this agreement.
Other agencies not listed above are also requested to sign the MARAC information sharing agreement and comply with the standards listed above and in the MARAC operating protocol document.