SG:
NHS
Police
- Council
- Partnership
'review
and do PLR

Edinburgh Violence Against Women Partnership

Information Sharing Protocol for the Multi Agency Risk Assessment Conference (MARAC)

Tracey - Data sharing
- Douglas to talk to NHS
- would it be app for women and up

covered by general info sharing protocol
{ Police
NHS - HV's
-

not covered.
Women Aid
Shakti
CEC - Housing
Comm safety
C+F - Educ WWM.
C+F
Adult Services
Substance misuse - Alcohol/Drug Recovery Service.
what do they have

Agreed:

Review:

Does protocol cover both general (pan Lothian Agreement) and specifics

Link to CAADA website
FAQ for info sharing
How do we ensure that clients fully aware of process.
Subject Access Requests.

- safe secure email (EDDACS)

Contents

Acknowledgements

This protocol was developed using guidance or protocols produced by CAADA and the London Borough of Richmond

Part 1 - Introduction

1.1 Purpose of this Protocol

1.1.1 The Edinburgh MARAC (or 'Multi-Agency Risk Assessment Conference') has been running in Edinburgh since April 2013. The MARAC is a meeting that brings together representatives from a number of agencies in Edinburgh to share information about the highest risk victims of domestic abuse. The intention is that this will enable agencies to jointly develop and progress appropriate and timely actions to make the highest risk victims (and any children) safer and to reduce crime and disorder. The MARAC is coordinated by the Domestic Abuse Sub Group of the Edinburgh Violence Against Women Partnership.

1.1.2 The objectives of the MARAC are:

- To share information to increase the safety, health and well being of victims, adults and their children;
- To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
- To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces the risk of harm;
- To reduce repeat victimization;
- To improve agency accountability; and
- Improve support for staff involved in high risk domestic abuse (DA) cases.

1.1.3 The purpose of this 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 (see below)
- To facilitate the exchange of information for this purpose;
- To clarify the understanding between signatories as to agencies responsibilities towards each other and data subjects;

1.1.4 This protocol is not designed to replace any existing data sharing protocols, but rather to enhance arrangements relating specifically to the exchange of information regarding domestic abuse.

1.1.5 This protocol sits alongside the Edinburgh MARAC Procedures, Protocols and Supporting Documents protocol for high risk victims of domestic abuse.

1.2 Agencies covered by this agreement

1.2.1 The following agencies are permanent attendees at the MARAC and are signatories to this Protocol:

Police Scotland
Criminal Justice Social Work
Lothian Health Board
Woman's Aid
Edinburgh Domestic Abuse Support Services
Safer Families
City of Edinburgh Council Children and Families
City of Edinburgh Health and Social Care Adult services
City of Edinburgh Education
City of Edinburgh Council Housing and Community Safety

Drugs and Alcohol?
Mental Health

1.2.2 Other agencies may be invited to become permanent MARAC attendees at a later date or to provide information to the MARAC where the MARAC considers this would be appropriate.

1.2.3 Other agencies may be invited to attend or supply information to the MARAC where there is one or more cases being discussed where they can provide relevant information on the case and assist in the development and execution of the risk management plan.

1.2.4 Any agency attending on this ad hoc basis will be asked to sign the MARAC confidentiality declaration at the beginning of the meeting.

1.3 Commitment

By declaring a commitment to the procedures set out in this protocol, signatories:

1.3.1 Will ensure that they are aware of their own organisations information governance procedures

1.3.2 Will ensure that data sharing arrangements between them are in compliance with the legislation laid out in *Appendix B*

1.3.3 Pledge to consult periodically with each other upon matters of policy and strategy.

1.3.4 Recognise that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller: a person within the partner agency who determines the purposes for which, and the manner in which, personal data are processed. The Data Controller will normally be the Designated Officer or Primary Designated Officer referred to in section 4 below.

1.3.5 Will not use the data received for any purpose other than that set out in this protocol, nor share it with any other party, without the disclosing partner's permission.

1.3.6 Undertake to ensure that they comply with all relevant legislation, this protocol, and any own internal policies on disclosure.

1.3.7 Agree to disclose information to relevant authorities under Section 115 of the Crime and Disorder Act 1998 - the police, local authority, probation or health authority, or to any persons acting on their behalf - where disclosure is for the purposes of a provision of the Act, and in accordance with any other relevant legislation. This agreement extends to those acting on behalf of a relevant authority to formulate or implement the Domestic Abuse Strategy.

1.3.8 Pledge to ensure that it is appropriately registered with the Office of the Information Commissioner for the purpose of sharing and receiving personal information for the purpose of crime reduction. Each party also pledges to ensure that the data it holds is as accurate and up to date as possible.

1.3.9 Will seek their own legal advice, wherever necessary.

1.3.10 Any signatory may withdraw from this Protocol upon giving written notice to the other signatories. Data which is no longer relevant should be destroyed or returned. The partner

must continue to comply with the terms of this Protocol in respect of any data that the partner has obtained through being a signatory.

Part 2 – Data

2.1 Data to be shared

Information may be shared at the MARAC about the following individuals:

- The victim(s) – this may include the new partner of a domestic violence perpetrator or previous partners;
- The children;
- The perpetrator (or alleged perpetrator); and where relevant to the risks posed, members of the perpetrator's family or people with whom he/she has other relationships.

2.2 Information which may be relevant and be disclosed

Information may relate to the victims, children and/or perpetrator and anyone else judged to be at risk

- Name (including any aliases), date of birth, address(es), ethnicity, sexual orientation, gender, gender identity;
- Details of police call outs, arrests, prosecutions, Court Orders, injunctions, bail conditions and other legal issues including immigration status;
- Relevant information held by a member agency on recent contacts (e.g. meetings, interviews, sightings, phone calls). This will include information on behaviour, demeanour, attitude etc;
- Relevant information on previous contacts, including those which may have occurred outside the city e.g. previous convictions, family or relationships history, substance misuse, mental health issues; and
- Any other information relating to the risks facing the victim and/or any other people who have been identified as being at risk.

2.3 Non-personal data

2.3.1 Signatory agencies understand that non-personal data is data that does not, nor has ever, referred to individuals. It will often be aggregate data and may be subject to the provisions of the Freedom of Information Act 2000, and there may be a duty to disclose this data to a third party if a request is made under the Act.

2.4 Depersonalised data

2.4.1 Depersonalised data encompasses any information that does not and cannot be used to establish the identity of a living person, having had all identifiers removed. Signatories recognise that great care must be taken when depersonalising data and that the Information Commission has stated that even a post-code or address can reveal the identity of an individual. Signatories are also aware that it may be possible for an individual's identity to be revealed by comparing several sets of depersonalised data.

2.4.2 Signatories accept that there are no legal restrictions on the exchange of depersonalised data, although a duty of confidence may apply in certain circumstances, or a copyright, contractual or other legal restriction may prevent the information being disclosed to partners. This is to be decided on a case-by-case basis by the disclosing agency.

2.4.3 It is best practice at the time the data is collected to give subjects information about how anonymised data about them may be used.

2.5 Personal data

2.5.1 Signatory agencies understand that personal data is 'information which relates to a living individual who can be identified from that data'.

2.5.2 Personal data will be clearly marked and kept securely within a pass-worded computer system or otherwise physically secure with appropriate levels of staff access.

2.5.3 Signatory agencies undertake to destroy all personal data when no longer required for the purpose for which it was provided.

2.5.4 All grounds for the disclosure of personal information under this protocol will be formally recorded, and partners will process information fairly and objectively in every case.

2.5.5 Agencies agree only to disclose sufficient information to enable partners to carry out the relevant purpose for which the data is required. This will be determined on a case-by-case basis, through negotiation between disclosing and receiving partners where necessary.

2.5.6 Signatories undertake that schedule 2 of the Data Protection Act 1998 and the Freedom of Information Act will be satisfied where it is necessary to process personal data.

2.5.7 Any record of domestic violence or information which may increase risk to a victim should be kept separately from notes held by the client to which the abuser may have access (for example, medical notes). This includes their address if living separately from the abuser, or any other information that could place the victim or child(ren) in danger.

2.6 Sensitive personal data

Sensitive data is that which falls into any of the following categories:

Criminal offences or proceedings;
Racial or ethnic origin;
Sexual life;
Physical or mental health;
Membership of a trade union; and
Religious or spiritual beliefs.

Part 3 – Data Sharing

The success of the MARAC hinges on effective and timely information sharing. It is recognised that families experiencing domestic abuse, and particularly those at highest risk, will need the help and involvement of a wide variety of agencies. This may include input from agencies working in the social, welfare, economic, safety, housing, criminal and civil justice sectors. Because of this a partnership approach is vital. Individual agencies will hold incomplete information about the family and this can inhibit the development of the most appropriate approach to managing risk. In contrast sharing information through the MARAC facilitates the development of appropriate and timely risk management plans.

Information shared at the MARAC will be used to draw up a safety plan which will, in the light of the information available and when put into practice, attempt to address the risks faced by the victim and children. In some cases it may also cover the risks faced by other people such as family members, colleagues or friends. Risks faced by staff working with the family may also be identified and included in the action plan.

3.1 Statutory Frameworks

The MARAC is just one of a number of different places where agencies will need to share information. Information sharing at the MARAC will take place within the framework provided by relevant legislation and guidance. Information can be shared provided each case brought to the MARAC meets the criteria outlined below:

3.2 Human Rights Act 1998

A disclosure to members of the same MARAC will comply with the HRA if it:

a) Is made for the purpose 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 these purposes; and
c) Complies with all relevant provisions of law including the DPA and the Caldicott Guidelines

3.3 Data Protection Act 1998

The prevention of crime exemption under the Data Protection Act means disclosure of information can be made to members of the same MARAC if it is necessary to prevent a crime against a named individual or a specified household.

3.4 Common Law Duty of Confidentiality

Under the Common Law Duty of Confidentiality, information given or received in confidence or for one purpose should not be used for another or passed to a third party without their consent

An obligation of confidence exists 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 clear duty of confidence the information can only be disclosed to 'third parties' if there is informed consent, compulsion of law or public interest.

3.5 Caldicott Principles

The guidelines state that where an individual has not consented to the use of their information that wish will be respected unless there are exceptional circumstances. Such an

exceptional circumstance is where there is a serious public health risk, risk of harm to the patient or other individuals or for the prevention, detection or prosecution of serious crime.

Practitioners should note that the Caldicott Guidelines are not law and that the DPA, HRA and common law will always take precedence.

3.6 The European Convention on Human Rights

Decisions to disclose must be necessary and proportionate, taking into account:

- The prevention or detection of crime, including safeguarding someone's life and/or child protection needs;
- If it is in the public interest;
- The right to life and to live free from inhuman and degrading treatment and torture; and
- If it is needed in order for confidential counselling, advice and support to take place

3.7 Local context for information sharing at MARAC

Within the City of Edinburgh, the majority of agencies involved in the MARAC will be signatories to a number of local information sharing protocols will share information in accordance with this framework.

It is the responsibility of individual agencies and their representatives on the MARAC to be aware of any particular legislation and/or guidance affecting their ability to share information. They should also be aware of internal procedures within their agencies for information sharing particularly where there is any doubt over whether information can be shared within the MARAC.

This information sharing agreement for the MARAC operates alongside existing local information sharing protocols.

3.8 Consent

It should not be assumed that consent is essential in order for agencies to share information.

Obtaining consent remains a matter of good practice and, in circumstances where it is appropriate and possible, explicit consent should be sought from and freely given by the data subject.

All agencies making referrals to the MARAC should have in place their own arrangements for ensuring that the victim and/or other family members where relevant, are made aware of the circumstances in which information about them will be shared and with whom.

Agencies should explain to victims:

- About their (ex) partner's limited confidentiality and what information they may or may not have access to;
- About their own confidentiality;
- About the agency's child protection policy; and
- How information is shared between workers at different organisations and within the organisation.

However, in many cases the aims of the MARAC might be prejudiced if agencies were to seek consent e.g. it may put the victim at greater risk if the alleged perpetrator discovered that the victim had given consent. In such cases the disclosing agency must consider possible grounds to override the consent issue. It is possible to disclose personal information without consent if this is in the defined category of public interest (see *section 3.2.1*).

Where consent is needed to share information about a young person (under the age of eighteen), it should be sought from the non abusive parent who has Parental Responsibility

(Section 2 (7) of the Children's Act 1989). Consent can be gained from only one person with Parental Responsibility, rather than both parents.

A young person (below the age of sixteen) can give consent in their own right if it can be demonstrated that they are of sufficient age and understanding to understand the implications and consequences.

Consent to share information will not be sought from the alleged perpetrator in order to protect the safety of the survivor. The perpetrator will not be informed about the meeting and the safety plan. Participants should take extraordinary care not to let the perpetrator know about any elements of the safety plan inadvertently.

Decisions to disclose without consent should be properly documented and identify the reasons why the disclosures are being made (i.e. what risk is believed to exist), the extent of any disclosures and the permitted use of the information.

For any cases where a decision is made to refer to the MARAC without consent, agency will have to complete an *Information Sharing Without Consent Form. (see Procedures, Protocols and Supporting Documents).*

Part 4 – Process

4.1 The MARAC meeting

At the beginning of each meeting all agency representatives will sign up to the MARAC Confidentiality Declaration which is that:

'Information discussed by the agency representative, within the ambit of this meeting is strictly confidential and must not be disclosed to third parties who have not signed up to the MARAC information sharing agreement, without the agreement of the partners of the meeting. It should focus on domestic abuse and child protection concerns and a clear distinction should be made between fact and opinion.
All agencies should ensure that the minutes are retained in a confidential and appropriately restricted manner. These minutes will aim to reflect that all individuals who are discussed at these meetings should be treated fairly, with respect and without improper discrimination. All work undertaken at the meetings will be informed by a commitment to equal opportunities and effective practice issues in relation to race, faith, gender, gender identity, sexuality and disability'

The information that is shared at the MARAC meeting will be used to construct a safety plan which will aim to address the risks faced by the adult victim and children.

Information on MARAC cases is sent out to members in advance of the meetings subject to the arrangements laid out in the Procedures, Protocols and Supporting Documents paper. No disclosures of information should be made to any other party, including the victim, without having been agreed at the MARAC. All decisions about how the information provided to the MARAC is to be used must be taken within the meeting. This includes both use by participants in the meeting and those outside the MARAC.

Cases coming before the MARAC will have been identified as being of the highest risk as defined by the MARAC referral threshold (using the Dash 2009 assessment tool) and should therefore meet the criteria for information sharing without consent.

The majority of cases will also involve children and so the requirement for information sharing for child protection purposes will, on most occasions, also come into force.

Failing to share relevant information can put victims and their children at serious risk. Bearing this in mind decisions by agencies to disclose information must still be justifiable given the estimated level of risk and should be proportionate.

Professionals representing their agency on the MARAC should decide what information they should disclose on a case by case basis taking into account the criteria given above and their own agency guidance. A decision to disclose a particular piece of information can be made in the context of discussions within the MARAC and need not necessarily be decided beforehand. For example a victim may have made one or more visits to their General Practitioner or Accident and Emergency. These may become relevant and the decision taken to disclose if it emerges these occurred around the same time as the police attended domestic violence incidents.

4.2 Information sharing outside of the MARAC

It may be the case that in order to implement certain elements of the MARAC action plan to manage risk persons who are not signed up to the MARAC information sharing protocol may need to be informed of certain facts. For example a perpetrator's name could be disclosed to a caretaker so that he would not be admitted to certain premise but the reason would not be given.

Considerations here are similar to those for sharing information within the MARAC. The risk of crime must be genuine or likely. If this is the case the Data Protection Act allows only the minimum necessary information to be disclosed by a MARAC agency to non MARAC recipients to allow a crime to be prevented.

Disclosures to persons outside the MARAC can still be permitted under the Human Rights Act. However members should satisfy themselves in advance that such disclosures are strictly necessary for the purpose for which they are being made.

4.3 Information sharing with other MARACs

4.3.1 In deciding whether to disclose information to another MARAC the principles set out in part 2 and 3 should be adhered to. This is addressed in *section 7.8 of* the Operating Protocol for the Richmond MARAC.

4.3.2 The initial disclosure by the referring MARAC should be restricted to the victim or perpetrator's name (and any children) and the fact they have been discussed at the Richmond MARAC. Recipient MARACs should have an information sharing protocol in place. Provided this is the case the Richmond MARAC will consider what additional information should be passed on, deciding what it can disclose and properly document the reasons for disclosure, what information will be disclosed and what restrictions are placed on the use of that information. This can include the completion of a referral form where requested by the recipient MARAC.

4.3.3 For urgent cases, occurring outside the MARAC meeting process, this action will be delegated to the Domestic Abuse coordinator or MARAC Administrator.

Part 5 - Security and Data Management

5.1 Data Controller and Responsibilities

5.1.1 Designated officers

Each signatory agency must appoint a Primary Designated Officer who will be a manager of sufficient standing and have a co-ordinating and authorising role. Agencies may also appoint further Designated Officers within the same body.

5.1.2 Responsibilities

Specific responsibilities will be:

- Ensuring their agency abides by the sections of this protocol;
- Ensuring that all Designated Officers and other staff are fully aware of their responsibilities;
- Appointing other staff in the body to act as Designated Officers in their absence;
- Authorising their agency's involvement and co-operation in the information sharing process, at every stage;
- Keeping a protocol co-ordination folder, which holds all the partner's information sharing documents;
- Ensuring their agency's Data Protection Notification entry is accurate, up to date and adequate for the purpose for which it is intended.

Criminal Justice Secure Mail (CJSM) exists to send confidential information by email to other organisations, which are also members of the secure email system. This service is run by the government's Criminal Justice Service on behalf of any public authorities, such as local authorities

Designated Officers and Primary Designated Officers are responsible for ensuring that processing of personal data is in accordance with the principles of the Data Protection Act 1998, namely:

- It is obtained, processed and disclosed fairly and lawfully;
- Kept securely;
- Processed in accordance with the rights of the data subjects;
- Accurate, relevant and held no longer than necessary;
- Disclosed only for a specified related purpose;
- Disclosed without the subject's knowledge and/or agreement only where failure to do so would prejudice the objective.

Designated Officers and Primary Designated Officers are responsible for keeping informed the data owners for each signatory agency. Only they can make formal requests and document agreements for the sharing of personal information under this protocol. They will also decide on a case-by-case basis when disclosure is necessary and when the public interest overrides the presumption of confidentiality.

They must also ensure ease of administration, covering all aspects and documentation of the information sharing process. This may be achieved by creation of a project folder or file, which must be kept up to date and include;

- Record of data disclosed;
- Project chronology;
- Project access list;
- Notes of meetings with partners;
- Recent correspondence and phone calls

5.2 Data Management

5.2.1 Partner agencies agree that it is their responsibility as signatories to this Protocol to ensure that they have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information we hold.

5.2.2 Partner agencies understand that there measures need to be taken to ensure the security of our partners and to protect the general public. It is the responsibility of each signatory to the agreement to ensure that their staff and any individual having access to information produced as a result of the MARAC receive sufficient training to enable them to handle such information and have been vetted to a satisfactory standard.

5.2.3 Personal information must be;

- Shared via Secure eMail using GCSX or the CJSM service2 when transmitted electronically. All partner agencies are responsible for ensuring they have this and health agencies, which have occasional links with the justice system. Organisations within the justice system itself (e.g. the Police and Probation Service) are already part of the Government Secure Community. For more information, go to http://www.cjsm.cjit.gov.uk/ . To use Secure eMail you must be using an email account from an organization within the Government Secure Community (e.g. .gsx, .gsi or .pnn); or an organization signed up to Secure eMail or anyone with an address ending .nhs.net facility. The MARAC Administrator will maintain list of the contact details of agency representatives, including their Secure eMail address.
- Be protected by back-up rules.
- When stored on a computer system be password protected or stored with restricted access.
- When manual, be stored in a secure filing cabinet when not in use.

- When manual, once paper copies have fulfilled their use they must be disposed of as confidential waste by shredding or other secure means.
- When manual, be located in a geographically secure environment.
- Not be inputted or accessed without industry standard devices as defined by BS7666.

5.2.4 All data held for the purposes of the MARAC is subject to a specified shelf-life of 3 years. Each agency that attends MARAC can hold relevant information for as long as a risk to the victim or children remains. The information retained should be proportionate to the perceived risk. All personal data disclosed will be held for this period. Particular care must be taken when agencies are disposing of old hard drives that have been used to store information relating to the MARAC. A suitably approved device must be used to wipe the memory clear or the hard drive must be physically destroyed to prevent third parties gaining access to this sensitive information.

5.3 Disclosure requests

5.3.1 Agreed procedures will generally require making a request in writing.

5.3.2 Access to information obtained through this protocol other than Primary Designated Officers and Designated Officers should be limited to employees whose work is directly related to the aim for which the data was obtained and those working within the crime reduction programme or field.

Subject Access Request

5.3.3 The data subject is legally entitled to request their records from the receiving agency under the Data Protection Act 1998, unless an exemption applies. If a subject requests access to their records the receiving agency should contact the disclosing agency to determine whether the latter wishes to claim exemption. From this stage the procedure should be fully documented in writing and stored on file.

Weeding of data

5.3.4 Signatories to the protocol must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice. Partners must agree a maximum retention period for data.

5.4 Publication

5.4.1 Where possible, this protocol should be published and made available to the general public for clarity of purpose. This publication will be subject to a regular review of information sharing protocols.

Media handling

5.4.2 Signatories agree when handling the media to ensure there is a consistent approach to media enquiries and that staff do not express personal views and respect the requirement for confidentiality and discretion. Partner agencies agree:

- to be fair to our fellow signatory agencies, and maintain their integrity;
- when providing information to the public, to do so honestly and fairly;
- statements must reflect the multi-agency decision process;
- consent of the data owner will be sought prior to release to the media;
- where practical, individual data subjects will be consulted if the media coverage was such that it may identify the individual.

5.4.3 This might be best achieved through development of a media strategy on a case-by-case basis, co-ordinated by the data owner.

5.5 Breaches

5.5.1 Partner agencies undertake at all times to comply with data protection and other legal requirements relating to confidentiality.
5.5.2 Partner agencies agree that any breach of confidentiality will seriously undermine and affect the credibility of the MARAC and broader partnership and information sharing arrangements and render us liable for breach of the law.

5.5.3 Any security breaches will be reported to the Chair of the MARAC, who is responsible for monitoring these. All agencies must have internal disciplinary policies in place for dealing with security breaches.

5.5.4 All parties to this agreement are aware that in extreme circumstances, non-compliance with the terms of this agreement may result in the agreement being suspended or terminated.

5.6 Audit

5.6.1 Partner agencies will ensure that they will collect, process, store and disclose all data held within the terms of the Protocol and the relevant legislation. Partner agencies agree to ensure that all information held is accurate, relevant and fit for the purpose for which it is intended.

5.6.2 Partner agencies agree to store all held data as securely as per the terms of Part 3 'Security'. Partner agencies pledge to conduct regular audits of their security arrangements to ensure they are effective.

5.6.3 The Community Safety Partnership undertakes to conduct annual audits of this protocol in order to amend it and ensure it remains fully effective

Part 6 - Complaints

6.1.1 Initial complaints must be referred to the appropriate Primary Designated Officer or Designated Officer.

6.1.2 The procedure to be followed in the event of a formal complaint being received is

- That the Chair of the MARAC is to be informed;
- Any formal complaint by a data subject regarding any stage of the process will be notified as a best practice measure in writing to all of our partners;
- Partner agencies will undertake to do all we can within the guidelines of the Data Protection Act 1998 to assist with any complaint.; and
- Individuals do retain the right to raise a complaint with such bodies as the Information commissioner or statutory ombudsman.

6.1.2 Initial complaints by one signatory agency against another signatory agency about their activity or processes must be referred to the Chair of the MARAC and the procedure to be followed in the event of such a complaint being received is as follows:

- Any formal complaint by a signatory regarding any stage of the process will be referred to the Community Safety Partnership Strategic Group
- Partner agencies will undertake to do all we can within the guidelines of the Data Protection Act 1998 to assist with any complaint.
- Individuals do retain the right to raise a complaint with such bodies as the Information commissioner or statutory ombudsman.

Appendix A: Signatories

The Chief Officers (or designate) formally agree to the following as permanent attendees at the MARAC:

- to subscribe to the principles contained in the Protocol;
- to work to the procedures identified within the Protocol
- to fully implement the protocol within their own agency, ensuring all staff know of its existence to support the MARAC, and to support their attendance at any training event required;
- to supply information within the bounds of this Protocol at no financial cost to any of the other signatory agencies; and
- to contribute to the development of trust and confidence between the signatory agencies by working within the framework of the protocol and Operating Protocol for the Edinburgh MARAC to disclose, retain and dispose of data for the purpose of supporting the MARAC.

DAIS (Drugs, Alcohol, Interventions, Support) and DIP (Drug Intervention Programme) Name
Signature
Date