Gloucestershire
Domestic Abuse

Multi Agency Risk Assessment Conference (MARAC)

Information Sharing Agreement

April 2008

Contents

Subject **Page**

Signatories to the Gloucestershire Domestic Abuse Information Sharing Agreement

By signing below, the participants accept and will adopt the statements included in this code of practice and the indemnity, and agree to maintain the specified standards.

Name	Post / Title	Organisation	Signature
Dr. T. Brain	Chief Constable	Gloucestershire Constabulary	
		Crown Prosecution Service Gloucestershire	
		Gloucestershire Children & Young People Directorate	
		Her Majesty's Courts Service Gloucestershire	
		Gloucestershire Probation Service	
		Gloucestershire Primary Care Trust	
		Gloucestershire Hospitals Trust	
		2Gether Partnership Trust	
		Gloucestershire Domestic Violence Support and Advocacy Project (GDVSAP)	
		Gloucestershire County Council	
		Cheltenham Borough Council	
		Cheltenham Borough Homes	
		Cotswold District Council	
		Fosseway Housing	

		Forest of Dean District Council	
		Gloucester City Council	
		Gloucester City Homes	
		Stroud and Vale District Council	
		Tewkesbury Borough Council	
		Severn Vale Housing	
		Stonham	
		Stroud Beresford Group	
		Victim Support Service	
		CAFCASS	
Peter Steel		Gloucestershire Drug & Alcohol Service	
		GARAS	

1. Parties/Signatories

Details of the chief officers / chief executives of the partner agencies who are signatories to this code of practice are shown on page 3 of this document.

It will be the responsibility of the signatories to this code of practice to ensure that:

- ethical standards are maintained;
- appropriate training is provided;
- the terms of this code of practice are adhered to.

2. Purpose

The purpose of this agreement is to facilitate the disclosure of data in order to comply with the statutory duty on chief police officers and local authorities to work together to develop and implement a strategy and tactics for crime reduction. This agreement will cover the disclosure of information between Designated Liaison Officers within the partner organisations and will relate only to incidents reported within the Gloucestershire area. This does not preclude information sharing outside of the area, where protocols are in existence or there are overriding issues of public safety e.g. perpetrators covered under MAPPA.

The signatories to this protocol are specifically concerned with the exchange of personal information in relation to the incidence of Domestic Abuse, and in particular victims identified as being at high or very high risk of harm, within Gloucestershire.

Domestic Violence/Abuse is defined as:

'*Any incident of threatening behaviour, violence or abuse (psychological, physical, sexual, financial or emotional) between adults who are or have been intimate partners or family members, regardless of gender or sexuality*.'

An adult is any person aged 18 years and over and family members are defined as mother, father, son, daughter, brother, sister and grandparents, whether directly related, in-laws or step-family.

Because victims' and children's safety issues and perpetrator accountability are so important, we will also apply our domestic abuse policy when dealing with criminal offences that occur in a **domestic context** involving victims and abusers **whatever their age**.

This information sharing agreement will work with the aims and objectives of Gloucestershire's Coordinated Community Response to Domestic Abuse(CCR); a multi-agency approach to reducing domestic violence. The aims of which are:

- To prioritise the safety of the victims and children.
- To hold perpetrators of domestic abuse accountable for their actions..
- To reduce repeat incidents of domestic abuse
- To emphasise community responsibility for confronting abusers and restricting their behaviour.
- To encourage Co-operation between organisations.

MARAC

The specific aim of Multi Agency Risk Assessment Conferences (MARACs), is to priortise the safety of victims who have been risk assessed at high or very high risk of harm, whilst also working with the aims stated above. .
The MARAC is an integral part of the Specialist Domestic Violence Court Programme, and information will be shared between the MARAC and the Courts, in high and very high risk cases, as part of the process of risk management.

‘

It is the purpose of this agreement to facilitate the exchange of information between partner agencies that will enable the partnership to fulfill its statutory duty and work together (Section 17 of Crime and Disorder Act 1998) to ensure public safety and for the prevention of crime and disorder. Specifically the aims are to achieve the following:

- reduce and manage risks to victims of domestic violence, in a multi agency setting to prevent and deter incidence of domestic violence.
- share personal information relating to individual incidence of domestic violence to enable actions by Partners that reduce the fear of crime (domestic violence).
- share information to support and encourage partnership working.
- share information relating to families experiencing domestic violence to enable work that reduces the impact of crime on children and young people.
- share information that will enable Partners to hold perpetrators accountable for their actions.

The signatories agree that working to the aims of Gloucestershire Domestic Abuse Coordinated Community Response is a measure for the prevention of crime and disorder.

3. Legislation and legal issues

The signatories to this code of practice agree to be bound by:

(a) the common law duty of confidentiality. Anyone proposing to disclose information not publicly available and obtained in circumstances giving rise to a duty of confidence will need to establish whether there is an over-riding justification for doing so. If not, it is still necessary to obtain the freely given, specific, informed and explixit consent of the person who supplied the information. This will need to be assessed on a case-by-case basis, and legal advice should be sought in any case of doubt. Guidance on what may constitute an ‘overriding justification’, or an overriding public interest is contained in section 4.2(b) of this code of practice.

(b) the Data Protection Act 1998 and its’ principles which require that personal data is:

- obtained and processed fairly and lawfully;
- processed for limited purposes;
- accurate, adequate, relevant and not excessive;
- not held longer than necessary;
- processed in line with data subject rights; and,
- kept securely.

(c) the Human Rights Act 1998 which states that everyone has the right to respect for his private and family life, his home and his correspondence, and that there shall be no interference by a public authority with this right except as in accordance with the law. The signatories to this code

of practice agree that the disclosure of personal data within this partnership may be necessary in certain circumstances to further the legitimate aims of ;

- ensuring public safety
- preventing crime or disorder
- protecting health or morals
- protecting the rights or freedoms of others.

(d) section 115 of the Crime and Disorder Act 1998 which allows for any person to disclose information to police authorities and chief constables, local authorities, probation committees, health authorities or persons acting on their behalf, so long as such disclosure is necessary for the purposes of any provision of the Act, i.e. the prevention of crime and disorder.

4. Disclosure of information

4.1 Depersonalised Data

This protocol is mainly concerned with the exchange of personal data where no other form of data will satisfy the requirement of personal data. When completely depersonalised information is requested, that is, information which does not readily identify the individual concerned by name or address or any other means, the assumption is that this information will be shared eg statistical information. If the purpose can be achieved using depersonalised information this is the recommended method. For undertaking an audit of crimes or incident numbers there is a presumption that management teams and consultative committees do not require personal data.

4.2 Disclosure of victim or witness details:

(a)**Consent:**

Before any personal data is disclosed to any of the signatories to this code of practice the specific, informed and explicit consent of the victim or witness should be sought. Many of the issues surrounding disclosure can be avoided if this consent has been sought and obtained. Consent must be freely given after the alternatives and consequences are made clear to the person from whom consent is being sought. As the data is classified as being sensitive, the consent must also be explicit. In this case the specific details of how the data will be used and disclosed, what information will be held, for what purpose and the reasons for any disclosure should be explained to the individual.

The victim or witness is entitled to withdraw consent at any time. Where a signatory is notified that consent has been withdrawn, that signatory must ensure that any other signatory to whom the details have been passed is notified in order for the removal and destruction of the data relating to that victim to take place.

(b)**Public interest:**

If explicit consent has not been sought, or sought and withheld, disclosure of personal details may still take place if there is an overriding public interest for the disclosure. Such a disclosure may **only** be made to a Stipulated Party. (see Appendix B “Definition of Terms”.)

When deciding if such an overriding public interest exists the following questions should be considered.

- Is the disclosure necessary for the prevention or detection of crime, prevention of disorder, to protect public safety, or to protect the rights and freedoms of others?

- Is the disclosure necessary for the protection of young or other vulnerable people?
- What risk to others is posed by this individual?
- What is the vulnerability of those who may be at risk?
- What will be the impact of the disclosure on the offender?
- Is the disclosure proportionate to the intended aim?
- Is there an equally effective but less intrusive alternative means of achieving that aim?
- Has the individual been informed that their information would be disclosed to the recipient?

It is intended that the individual with responsibility for convening a MARAC (Divisional Detective Inspector) will write to inform victims that they have been identified as being at high or very high risk of serious harm from domestic violence related crime, and that it is necessary to share this information within a MARAC. This letter will also inform the Victim of the role of the Independent Domestic Violence Advisor. See Appendices B & E

The disclosure of personal data without the consent of the person to whom it relates is a serious step. Before any such disclosure is made, approval should be sought in writing from a senior official of the agency proposing to disclose. In the case of Gloucestershire Constabulary this should be an officer of the rank of superintendent or above Note R v Chief Constable of North Wales ex parte see Appendix D

4.3 Disclosure of suspected offender details:

Section 115 of the Crime and Disorder Act 1998 provides that the signatories to this code of practice have the power to make disclosures of personal information to Stipulated Parties where this is necessary or expedient for any provision of the Crime and Disorder Act, including section 17, the duty on local authorities to exercise all functions with due regard to prevent crime and disorder.

The Data Protection Act 1998 maintains the crime prevention exemptions of the Data Protection Act 1984. Disclosure may be made to any agency or authority where it is for the purpose of the prevention or detection of crime, apprehension or prosecution of offenders, **and** where failure to disclose would be likely to prejudice those purposes. **However, any decision to disclose personal information must be made on a case by case basis,** (S.29(3), Data Protection Act 1998).

5. Specific safeguards - personal data exchange

5.1

a) The decision to exchange Personal Data between partner agencies will be made on a case by case basis, by the holder of the information. Disclosure may be made despite a duty of confidentiality, where there is an overriding public interest, see para 4.2.(b) of this code of practice. **Information holders will not be under a duty to disclose nor will potential recipients have any power to demand disclosure**.

b) If there is any doubt whether the request for information falls within the Personal Data category, the issue should be referred to the Data Protection Officer for the

Stipulated Parties concerned for advice and guidance.

c) Should information be disclosed in order to achieve the objectives of the Crime and Disorder Act 1998, this agreement specifically excludes the recipient of the information from using the received information for their own secondary purposes.

To enable the requesting organisation to make the most informed, considered and effective decisions regarding the appropriate course of action in any specific case, information will need to be exchanged at the earliest possible opportunity.

d) It is very important to ensure that the confidentiality of data subjects is maintained at all times, unless there is an overriding public interest to disclose the specific personal data involved in identifying those who are actively involved in crime or anti social behaviour. Extreme care needs to be taken to ensure that victims, witnesses, or complainants are never identified. This is particularly important in cases of domestic violence due to the unique relationship between the victim and perpetrator.

5.2 Designated Liaison Officers

a) In order to ensure that personal information is exchanged in the most efficient, effective and secure manner, each signatory to this code of practice will select and appoint Designated Liaison Officers who will be authorised to request and disclose personal data. A list of nominated liaison officers will be compiled by each signatory and circulated to all members. In doing so, partner agencies must only identify the minimum number of officers in order to retain operational effectiveness, dependent on the size and structure of the specific organisation.

Information holders will not consider requests for information- other than that requested by Designated Liaison Officers.

b) The Designated Liaison Officers are expected to have received appropriate training in relation to the provisions of the Data Protection Act 1998. In specific terms, the Designated Liaison Officers should be fully conversant with the following:
   - the Data Protection Principles particularly issues relating to lawfulness and fairness;
   - in what circumstances the duty of confidentiality can be overridden;
   - roles and responsibilities of Data Controllers and Data Processors and,
   - the contents of this code of practice.

c) Information, which has been disclosed to achieve an objective of the Crime Disorder Act 1998, will be retained by the Stipulated Parties and other parties for no longer than is necessary to achieve that specific objective. In any event information will not be retained longer than five years after the case has been finally disposed of, unless other relevant proceedings are commenced within this period.

d) Information should be factually relevant, i.e. the minimum amount of personal non-anecdotal information should be retained which is necessary to achieve the specific objective under the Crime & Disorder Act 1998. In the case of MARACs under this agreement, the only information retained will be:-
   - the dates of incidents and convictions*;*
   - personal details of victim, perpetrator and children;
   - details of level of risk to victim from perpetrator of Domestic Violence.

- details of actions taken by any agency in relation to Domestic Violence;
- details of location to which any Domestic Violence related Order relates;
- any other conditions attached.

e) Information to be kept must be accurate. Information retained by Stipulated Parties and other parties should be regularly monitored and corrections or amendments made known to the Stipulated Parties which also retain that particular information.

f) Security of data: Each partner must ensure that they have appropriate security arrangements in place and take all reasonable steps to adequately protect data from both a techological and physical point of view. In accordance with British and International Standards BS ISO/IEC 27001:2005 (Information technology security techniques and information Security Management System) and BS7799-2:2005 Code of Practice for Information Security Management. This must include security of computer data, manual files and all forms of transfers of data between partners, including handwritten notes taken at MARAC meetings. Each partner must state:

- Who can access what information
- Who makes disclosure decisions
- Where date/information is stored

g) If information is being transferred by post or courier it must be sealed and double enveloped, fully addressed, return address on outer envelope and sent recorded delivery. Internal despatch should be doubled enveloped, fully addressed, return address on outer envelope, and acknowledgement receipt sent either by telephone or email to sender. Hand delivered documents should be treated in the same way as internal despatch.
No information will be sent by fax, as this is no longer considered a secure method of sending information.

h) If e-mailing Government approved encryption is required.

i) WAP phones / pagers are not to be used

j) The Data Protection Officer for each Stipulated Party may undertake compliance audits of any issues described in this code of practice.

k) Copies of documents and printouts from the Police National Computer and other databases will not be supplied to other agencies. Relevant information will be transcribed onto a word document or other written communication before being exchanged. The Divisional Detective Inspector responsible for convening and chairing the MARAC will decide what is recorded in the minutes of the meeting. These minutes will officially record the information that was agreed to be shared.

5.3 Data Quality

The signatories agree that they will be responsible for ensuring that the data which each party supplies is both accurate and up-to-date. Where accuracy of data cannot be guaranteed the provider will ensure that all recipients are made aware.

Information discovered to be inaccurate or inadequate for the purpose will be notified to the data owner who will be responsible for correcting the data and notifying all other recipients of the data who must ensure that the correction is made.

5.4 Previous Convictions

The responsibility for disclosure of validated previous convictions will rest with the National Criminal Records Office.

In the case of requests for disclosure of previous convictions for the purposes of legal proceedings, the Designated Police Liaison Officer will contact the Criminal Records Office on behalf of the requesting Organisation.

The Criminal Records Office can then communicate the validated criminal record directly to the legal representative of the Stipulated Party involved.

Care must also be taken to ensure that "spent" convictions, within the meaning of the Rehabilitation of Offenders Act are not disclosed.

5.5 Administration

a) All disclosures of information will be recorded and documented in accordance with Forms approved for use by the Stipulated Parties as follows (see Appendix F):
    1.

b) Information holders will not seek any financial contribution from the recipient. It should be noted that Conduct Money, which is mandatory under the Magistrates Courts Act 1980, will still be paid in circumstances when witnesses are summoned to attend court proceedings to give evidence or to produce documents.

This protocol will be made available to members of the public and other interested bodies. It will be reviewed annually by each Stipulated Party.

6. Security

6.1 Security Statement

Each partner agrees to abide by the baseline security statement detailed at appendix C. Breaches of security shall be dealt with in accordance with this appendix.

6.2 Data Protection Officers

Each partner to this agreement will designate a person of appropriate rank within their organisation to assume responsibility for data protection (including notification if appropriate), security and confidentiality; and compliance with legislation, e.g. by undertaking audits at regular intervals. Details of each partner's nominated data protection officer are shown in appendix A

6.3 Indemnity

In consideration of the provision of information in accordance with this agreement each signatory undertakes to indemnify each and every signatory to this code against any liability which may be incurred by such signatory as a result of the provision of such information or by any breach of this agreement.

Provided that this indemnity shall not apply:

(a) where the liability arises from information supplied which is shown to have been incorrect, unless the signatory claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part.

(b) unless the signatory claiming the benefit of this indemnity notifies the authority granting indemnity as soon as possible of any action, claim or demand to which this indemnity applies, permits that partner to deal with the action, claim or demand by settlement or otherwise, and renders that partner all reasonable assistance in so dealing.

(c) to the extent that the signatory claiming the benefit of the indemnity makes any admission which may be prejudicial to the defence of the action, claim or demand.

7 Complaints and Breaches

7.1 Any complaint made by an individual concerning the disclosure of data by one signatory to any other signatory of this code of practice will be brought to the attention of the nominated officer of the relevant signatory. Such complaints will then be dealt with in accordance with that signatory's own policies and procedures. Where it is relevant to do so, signatories will keep each other informed of developments following a complaint.

Where a complaint is made about the disclosure or use of information from a police system, this will be brought to the attention of a police officer of at least the rank of Inspector.

Persons making a complaint should be informed of their right to raise the matter with the Information Commissioner or a statutory ombudsman.

7.2 Any further guidance reviewed annually and distributed via the holder of this agreement should be considered for attachment tothe agreement.

8. Subject Access

Individuals have the right of access to a copy of all information held about them on computer and manual files(Subject access), unless an exemption applies where information can be withheld under certain circumstances. The Data Protection Act 1998 requires that all subject access requests are dealt with within 40 days.

All such subject access requests should be brought to the attention of the nominated Data Protection Officer as soon as they are received. All partners should have a written Subject Access Policy, with procedures in place for staff to deal with such requests.

If an agency receives a subject access application and personal data is identified as belonging to another agency, it will be the responsibility of the receiving agency to contact the data owner to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act. Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless: -

(a) The other individual has consented to the disclosure of the information to the person making the request, or

(b) It is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to;

- any duty of confidentiality owed to the other individual,
- any steps taken by the data controller with a view to seeking the consent of the other individual,
- whether the other individual is capable of giving consent, and
- any express refusal of consent by the other individual.

Appendix A.

Gloucestershire Domestic Abuse Information Sharing Agreement - Data Protection Officers.

1. Organisation	2. Address	3. Tel / Fax	4. Data Protection
Gloucestershire Constabulary	Gloucestershire Constabulary No.1 Waterwells Waterwells Drive Quedgeley Gloucester GL2 2AN	– 0845 0901234	Data Protection Officer, Police HQ

Dated : _____ Day of _____, 2008_

Appendix B.

Definition of terms

Personal data: Data which relates to a living individual who can be identified

- a. from that data, or
- b. from that data and other information which is is the possession of, or is likely to come into the possession of, the data controller.

Stipulated parties: Relevant Authorities as defined by section 115 of the Crime and Disorder Act 1998, i.e.:

- a chief officer of police,
- a police authority,
- a local authority,
- a probation committee,
- a health authority,
- bodies which must co-operate under the Crime and Disorder Act Section 5 (2) (c), i.e. Registered Social Landlords, Parish / Community Councils, NHS Trusts.

Crime: an act, default or conduct prejudicial to the community, the commision of which, by law, renders the person responsible to punishment by a fine, imprisonment or other penalty.

Designated liaison officers: trained representatives of the **stipulated parties** who are the contact point for the exchange of data between such parties and managing the associated administration systems.

Applying powers of arrest in domestic violence cases:
On 1 January 2006, the Serious and Organised Crime and Police Act 2005 (SOCPA) introduced amendments to the Police and Criminal Evidence Act 1984 (PACE) which alter police powers of arrest. These amendments supersede section 10 of the Domestic Violence Crime and Victims Act 2004, which would have given a power of arrest in common assault cases. Now officers have the power to arrest for any offence, but must demonstrate that they have reasonable grounds for believing that the arrest is necessary for one of the reasons listed in PACE section 24 (as amended by SOCPA section 110(1).
Where an offence has been committed in a domestic violence case, arrest will normally be 'necessary' within the terms of SOCPA to protect a child or vulnerable person, prevent the suspect causing injury and/or allow for the prompt and effective investigation of the offence. Proactive investigation will always be required in cases of domestic violence as the victims, children, neighbours and other witnesses may be reluctant to disturb the perceived privacy of family life. They might also fear threats, emotional pressure and violent reprisals from suspects.
Code G of the PACE Codes of Practice states that an arrest to allow prompt and effective investigation may take place for a number of reasons, including where there are grounds to believe that a person may intimidate or contact witnesses.

-

Multi Agency Risk Assessment Conferences (MARACs): Are Police convened meetings that are held in the Victim's name to manage and reduce risks. Only victims identified as being at high or very high risk of serious harm will be included in the MARAC process. The MARAC is an integral

part of the Specialist Domestic Violence Court Programme, as information shared at MARAC will be shared with Crown Prosecution Service, to aid prosecution of cases. An expected outcome of MARAC working closely with the Specialist Domestic Violence Court is that convictions for Domestic Violence related crime will increase, and that risks experienced by Victims will be reduced. An intrinsic part of the MARAC process is multi agency working and information sharing. It is only in this way that a broad view of what is actually happening for the Victim can be gained, and then a more accurate assessment of risk made and a multi agency risk management plan built.

Independent Domestic Violence Advisor (IDVA) The role of the IDVA is to work with Victims identified at high or very high risk of harm, within the MARAC process. This role will act as link between MARAC, Victims and Courts, by providing support to the victim through the process, safety planning ; liaison with court staff; referrals to other agencies as appropriate.

Risk Evaluation

Risk in domestic abuse cases is assesed according to the presence of key risk factors. These are captured by means of a risk assessment checklist and can be carried out by any agency. See Appendix

To whom the risk can be associated with: (MARAC)

- A known adult: such as current or previous partner
- Children: who may be vulnerable to harm of various kinds, including violent or sexual behaviour, emotional harm or neglect.

Appendix C.

Gloucestershire Domestic Abuse Information Sharing Agreement

Baseline Security Statement

The following are Baseline Security measures, which all partners will make sure, are in place to protect the information. These may be supplemented by additional arrangements according to circumstances.

The **Baseline Measures** are:

1. Information Security Policy. Each partner will ensure they have a statement of Information Security Policy, which confirms its commitment to the protection of the information.
2. Protection levels. The protective security measures imposed shall be appropriate to the sensitivity of the information. For Gloucestershire Constabulary this means in accordance with the measures applicable to RESTRICTED information as defined in the Government Protective Marking Scheme (GPMS). For Partner Agencies, which have not adopted GPMS this means in accordance with the measures applicable to CONFIDENTIAL information as defined in, documented organisational polices.

3. Personnel. The reliability of those with access to the information will be assessed by ensuring that all personnel with access to data have a current CRB check, confirmed by their employer. The people who have access to the information will be trained in security and data protection, and this training will include the procedure for reporting security incidents or breaches. People with access will be asked to sign a Confidentiality/Non-Disclosure Agreement at every MARAC that they attend.
4. Physical Security. Measures will be in place to prevent unauthorised access to the information. This includes control of access to the buildings and rooms where the information is processed. The information will be stored in lockable cabinets and access to the cabinets will be restricted to authorised persons only dependant upon the quantities held a second barrier i.e. a lockable cabinet within a locked room may be required. The information will be transmitted by secure means as described in paragraph 5.2 above The information may not be transmitted via the Internet unless Government approved encryption is used.
5. Sensitive waste. Waste documents must be shredded, use secure sacks and keep secure when unattended i.e. the final disposal should be made via a third party provider or within own resources ensuring waste is burned or pulped it should not be placed into the general waste Floppy disks – dismantle and cut into small pieces, dispose with normal waste. CD Roms – destroy completely- disintegrate, pulverise, melt or shred.
6. Computer management. Only authorised persons may access computer systems that store or process the information. Access may be audited. Appropriate anti-virus precautions must be in place. Documented system security rules and procedures will be in place.
7. Business Recovery/Continuity. The computer systems that process the information will be backed up, and copies of the information stored on appropriate backup media, for use in restoring the system in the event of a disaster.

Security Incidents and Breaches

Reporting Procedure

Definition: A security incident is any suspected failure in information security, namely:

- deliberate or accidental unauthorised disclosure of information;
- deliberate interference with the availability of a system or systems;
- accidental or deliberate destruction of information;
- accidental or deliberate modification of information;
- unauthorised systems access;
- misuse of information;
- theft of assets;
- any other event affecting information security.

The named officer with Partner agency with responsibility for information security will also have responsibility for investigating any suspected failure in information security. In the first instance details of the incident should be reported to the named officer who has responsibility for information security. It is the responsibility of the named officer to ensure that details of any information failure is reported to other partner agency named officers if this is likely to affect the information security in there organisation.

Details of the incident must include:

- Date and time of the incident;
- Type of incident e.g. computer access
- Person reporting;
- Any other persons involved;
- Details of the incident;
- Current state as a result i.e. the effect of the incident.

3. The Named Officer shall initiate an investigation into the incident. Other specialist departments may be involved at the request of the Information Security Officer e.g. the Police Internal Investigation Unit, in accordance with Constabulary procedure.

4. The named Officer will liaise closely with the Partner's officer and will determine and agree any immediate amendments to security arrangements or policy. The Officers will notify their own management in accordance with their organisation's own rules and procedures.

6. At the end of the investigation, the named Officers will produce a report of the incident, which will include any recommendations for improvements to security arrangements or policies as a result of the incident. A record of the incident and subsequent result will be kept by the Information Security Officers.

APPENDIX D

YEAR OF CASE **R v CC OF NORTH WALES POLICE**

YEAR OF CASE YEAR 1998

COURT Court of Appeal

CASE NARR This case was heard at the Court of Appeal on the 18th March 1998. The Court basically approved the following decision made by the Queen's Bench Division.

AB and CD were a married couple, recently released from prison after serving sentences for serious sexual offences against children. In the winter of 1997 they hired a caravan on a holiday site in North Wales. The police were very concerned that when the site opened to holidaymakers at Easter, children playing on the site might be vulnerable to attack by the couple.

After discussions with the couple, a psychiatrist and other agencies, such as social services, it was decided to inform the site owner of the couple's convictions. The owner made them leave.

The couple brought an action for judicial review of the police's conduct.

HELD

In LIMITED circumstances the police could release factual information about individuals if it was very strongly in the public interest to do so.

The Court approved the Home Secretary's instructions to the police concerning the release of such information. They say:

1. There is a general presumption that information should NOT be disclosed, such a presumption being based on a recognition of:
    - the potentially serious effect on the ability of the convicted people to live a normal life;
    - the risk of violence to such people; and
    - the risk that disclosure might drive them underground.
2. There is a strong public interest in ensuring that the police are able to disclose information about offenders where that is necessary for the prevention or detection of crime, or for the protection of young or other vulnerable people.
3. EACH CASE SHOULD BE CONSIDERED CAREFULLY ON ITS PARTICULAR FACTS (there must be no blanket policy), assessing the risk posed by the individual offender; the vulnerability of those who may be at risk; and the impact of disclosure on the offender. In making such an assessment, the police should normally consult other relevant agencies (such as social services and the probation service).

Appendix E

Gloucestershire Multi Agency Risk Assessment Conference (MARAC)

CONFIDENTIALITY DECLARATION

Date:

The Chair of the meeting reminds all concerned of the Protocols within the agreed Gloucestershire Multi Agency Risk Assessment Conference (MARAC) Information Sharing Protocol.

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 Information Sharing Protocol, without the agreement of the partners of the meeting. This includes Victim, Perpetrator and other third parties.

All agencies should ensure that the minutes are retained in a confidential and appropriately restricted manner. Any partners should be aware that the Information Sharing Protocol also binds any handwritten notes. These Minutes will represent the agreed shared information. 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, Gender, Sexuality and Disability.

The purpose of the meeting is as follows:

1. To share information to increase the safety, health and well being of victims – adults and their children;
2. To determine whether the perpetrator poses a significant risk to any particular individual or to the general community;
3. To construct jointly and implement a risk management plan that provides professional support to all those at risk and that reduces risk of harm;
4. To reduce repeat victimisation;
5. To improve agency accountability;
6. Improve support for staff involved in high and very high risk DV cases.

The responsibility to take appropriate actions rests with individual agencies; it is not transferred to the MARAC. The role of MARAC is to facilitate, monitor and evaluate the effective information sharing to enable appropriate actions to be taken to increase public safety.

By signing this document we agree to abide by these principles.

Gloucestershire Multi Agency Risk Assessment Conference (MARAC)

CONFIDENTIALITY DECLARATION

Date:

Name	Agency	Signature

Appendix F MARAC Forms

MARAC Admin Pack can be downloaded from CAADA website
www.caada.org.uk/library_resources.html#10