

April 2008

# **RISK OF HARM PROTOCOL**

**2008**

## CONTENTS

### AGREEMENT TO THE SHARING OF INFORMATION PROTOCOL

#### Part A – The Protocol

#### Part B – Technical Details

1. INTRODUCTION
  2. THE PROTOCOL – STATEMENT
  3. PRACTICAL POINTS
  4. SPECIFIC REMIT
  5. TECHNICAL ‘KNOW-HOW’ TO OPERATE THE PROTOCOL
    - a) Working Definitions
    - b) Basic Principles Regarding Risk
    - c) Disclosure – Legal Context and General Guidance
  6. APPLICATION LEVELS OF PROTOCOL
    - a) Routine Operational Exchanges
    - b) Broad Risk Assessment
    - c) Specific Risk Management
    - d) Potentially Dangerous/High Risk Cases
  7. APPLICATION FOR PROTOCOL
  8. MONITORING THE IMPLEMENTATION OF THE PROTOCOL
- 
- |         |   |
|---------|---|
| Annex A | Multi Agency Public Protection Panel Processes  |
| Annex B | Vulnerable Adult Procedure                      |
| Annex C | Risk of Harm Disclosure Checklist               |
| Annex D | Procedure for Lateral Checks                    |
| Annex E | Determining the Public Interest                 |
| Annex F | Young People                                    |
| Annex G | Criminal Procedures and Investigations Act 1996 |
| Annex H | sharing of Information Indemnity Form           |

## 1. INTRODUCTION

Acting under the imperatives of the Safer Communities Legislation, the protocol was commissioned by the Warwickshire Community Safety Partnership and Drug Action Team (WCSP & DAT). It is an agency-level agreement that empowers professionals working in these agencies to exchange information with each other **relating to adults and young people:**

- Who are harmful, or who are likely to be harmed
- To identify means of jointly managing the risk of harm

Each signatory agency has affirmed commitment towards public safety and agrees to adhere to the undertakings and principles contained in the protocol.

This protocol will come into effect on DD. MM. YYYY and will be reviewed annually thereafter.

Any amendments to this protocol made before the next review date, will need to be approved in principle by all partner organisations and will only be effective until the review date. All amendments will need to be ratified and endorsed by the partner organisations and their legal departments at the review date.

## 2. THE PROTOCOL – STATEMENT

The decision to share information under this protocol remains the responsibility of individual agencies. Each agency must adhere obligations it holds under statutory legislation and common law. In particular, this includes the Data Protection Act 1998, the Human Rights legislation, and any duties and obligations held under common law.

To override an individuals confidentiality rights, there has to be an overriding need to protect the safety of potential victims and the community from the risk of harm.

No agency will retain information it does not need that it has received from another agency in the course of a risk assessment.

## PART B – TECHNICAL DETAILS

### 3. PRACTICAL POINTS

Each agency must continue to make its own decisions and meet all of its own legal obligation with respect to information and the management of the particular circumstances of risk. The protocol does not involve any new legal powers about giving or receiving information, but it does confer professional empowerment in limited areas of risk.

This protocol is entirely separate from child protection procedures. **Wherever child protection concerns relating to identified children are present, then the Warwickshire Child Protection procedures should be used.**

The protocol has to be considered alongside three other sources of guidance in Warwickshire which address risk:

- The Warwickshire Inter Agency Child Protection Guidelines (see the “blue book” which is issued separately)
- Multi Agency Public Protection Arrangements procedures (See Annex A)
- Vulnerable Adult Procedures (See Annex B)

#### 4. SPECIFIC REMIT

This protocol refers to the sharing of information about adults and young people who present a risk to: -

- The community
- Specific Potential Victims
- Professionals

The following are good examples of where the protocol is designed to help:

- An individual is believed to present a risk of physical danger to an individual or the general community and it is necessary to be able to share information with another agency to protect the community and a potential victim from any harm.
- A new risk assessment has to be completed with respect to an existing offender in order to cope with a changed risk, and to do so it is necessary to check information held by other agencies.
- A victim is at risk of significant harm and it becomes necessary to breach their own confidentiality in order to protect them from that harm.
- An individual presents a risk to other professionals who need to be made aware of possible risk and danger.
- In order to protect a vulnerable person an agency needs to make a limited disclosure to a member of the public.

The protocol is not designed for use in these two circumstances with Children and Young People:

- Where a specific child is believed to be at risk of significant harm (Child Protection Procedures apply).
- Where a young person (under sixteen years of age) presents a risk of significant harm to other children (Child Protection Procedures – Section 5.9 apply)

## 5. TECHNICAL 'KNOW-HOW' TO OPERATE THE PROTOCOL

- 5.1 The Protocol deals with “reducing the risk of harm”, and it does so in the belief that maintaining the safety of the public and the community is compatible with meeting the needs of an individual.
- 5.2 It does this by facilitating information sharing as part of the overall management of the risk and of all vulnerable parties – offenders, community and professionals.
- 5.3 To gain an accurate assessment of the nature and level of risk an individual presents it is frequently beneficial, and sometimes essential, to share information between agencies. The information that one agency holds may appear insignificant in isolation but becomes critical when it is placed alongside the information held by another agency.
- 5.4 Risk cannot be eliminated, but if agencies work together with approved policies and procedures to address risk, they may be able substantially to reduce harm in certain cases and ensure better protection for the community.
- 5.5 Those using the Protocol will find it helpful to have the following key ideas defined. Crime is defined by law, and its impact is gauged from the perspective of the particular local community at that time and place.

### A) Working Definitions

#### 5.6 Risk Assessment

To establish the level of risk posed it will be necessary to exchange information on a range of individuals and this information may be stored where there is a justification to do so. The protocol, therefore will lead to information being exchanged on people who eventually are not assessed as high risk in some cases.

#### 5.7 Self-Harm

Apart from the accepted professional usage of this term in situations of deliberate self-harm, the Protocol recognises two additional aspects:

- That planned self-harm may also cause risk of harm to others
- That some stage of the self-harm process is likely to come to the attention of an agency, not your own, which may be able to instigate further harm reduction if information can be shared in timely way.

#### 5.8 Agency

The professional activities of employees of organisations who are signatory to the Protocol.

#### 5.9 Crime

Crime is any act that is deliberately done, or deliberately not done, where the consequences is prejudicial to the safety of the community and the act would be sufficient for the law to render the perpetrator liable to

punishment – by a fine, imprisonment, or other penalty. This definition includes domestic violence.

**5.10 Psychological Impact**

When the perceived level of risk to a victim from an individual's behaviour could be regarded as falling within the remit of the Protection from Harassment Act 1997.

**5.11 Anti-social behaviour**

Anti-social behaviour means acting in a manner, which causes or is likely to cause harassment, alarm or distress to one or more persons not of the same household as himself.

**5.12 Disorder**

Disorder refers to the level or pattern of anti-social behaviour within the context of a particular geographical area.

**5.13 Racist Incident**

A racist incident is any act that is perceived to be racist by the victim or any other person (Macpherson Report).

**B) Basic Principles Regarding Risk**

5.14 All agencies and their employees must be aware of risks and risk management. Professional officers need to be alert to signs of high risk and be aware of their responsibility to protect themselves, other staff, and the local community from harm.

5.15 Agencies and their employees are therefore expected:

- To take seriously concerns (informally or formally raised, anonymous or otherwise) regarding individuals who may threaten others in the community.
- To keep an open mind which does not prejudge the situation. This applies equally to concerns raised by or regarding the family of the individual in question.
- To investigate risks in an effective manners.
- To share information as specified in this Protocol
- To offer best possible protection to the potential victim, the individual giving cause for concern and the community. This means keeping a balance between acting responsibly in relation to the individual who presents the risk, on the one hand, and protecting the public from harm and maintaining safety in the community on the other, bearing in mind that Public Safety overrides all other considerations.
- To work co-operatively with other agencies, where the combined benefit will be greater than that achieved separately by each agency.
- To undertake internal inquiries if major incidents, involving death or serious injury take place. The purpose is to learn from experience and to share that learning with other agencies.

### **C) Disclosure – Legal Context and General Guidance**

- 5.16 Public Protection overrides the general policy of confidentiality in respect of personal information. Each decision involving whether or not to disclose, should then be justified by the likelihood and impact of the harm that disclosure will prevent.
- 5.17 The legal context within which disclosure decisions have to be taken is continually evolving and the Courts remain the ultimate authority on the circumstances of what and how information can be disclosed by the Police and other agencies. For example, some or all of these separate area of law may have a bearing on disclosure in any specific case:
- The common law of duty of care
  - The common law of duty of confidence
  - The Data Protection Act 1998
  - The European Convention of Human Rights – especially the right to the protection of private and family life and the principle of proportionality
  - The law on defamation
  - The Children's Act 1989 – which provides a framework for the care and protection of children
  - The Crime and Disorder Act 1998
- 5.18 Most contemplated disclosure will be limited to informing individual officers on a need to know basis, particularly in other agencies.
- 5.19 But there may be occasions where an agency has to make a disclosure to a member of the public to protect a particular individual. This should only be taken in exceptional circumstances.
- 5.20 In most cases this will take place after a multi-agency risk assessment has been completed, and the disclosure has been agreed as part of the management plan. However, there are some cases and situations when agencies have to act in the public interest outside of multi-agency meetings and make disclosure after carefully consideration of the consequences both to the potential victim and the individual who presents the risk.
- 5.21 There is inevitably some risk of legal action relating to any disclosure, and in some circumstances notifying an individual that disclosure of their personal information is to be made will cause them to modify their dangerous behaviour, this defusing the situation.
- 5.22 For specific guidance about disclosure to another agency, see the Disclosure Checklist in Annex C.

## 6. APPLICATION LEVELS OF THE PROTOCOL

6.1 This agreement about the sharing of personal information applies at all levels of contact between agencies in order to best protect staff and other vulnerable individuals. It covers everything from verbal exchanges between officers to the formal holding and storage of written information.

6.2 The four main levels of information are as follows:

### A) Routine Operational Exchanges

This would be where professional officers exchange information during the course of their daily activities:

- For example, a Community Psychiatric Nurse or Bail Information Officer entering a Police cell could reasonably expect to be told by a Custody Sergeant if there is any risk, or vice versa.
- Medical staff admitting a patient could reasonably expect to be told by the referring agency if there is a history of violence.
- A Housing Officer could reasonably expect, as part of the referral, to be told of any pertinent risk to themselves or the community which may affect the interview arrangements or decision about where to re-house.

**The intention of the Protocol at this level is to regularise the existing process of professional verbal exchange of necessary information.**

### B) Broad Risk Assessment

This would be where a professional officer in an agency responsible for an individual – as a patient, suspect etc – has concern about the safety of others and is collecting information to complete a risk assessment. In the process they will make direct contact with other agencies or workers to establish if they are known and whether there are any risk factors.

**The intention of the Protocol at this level is to broaden the level of understanding about the situation or about the individual in order to better inform decisions.**

### C) Specific Risk Management

This would be where a professional officer in an agency responsible for an individual – as a patient, suspect etc – has identified a worker in another agency who is also involved in the case and with whom there is a need to share information in order to co-ordinate the work and share the responsibility. The level of risk may vary in these cases, the emphasis being on joint management of a situation where more than one agency has a statutory responsibility for a potentially dangerous situation.

**The intention of the Protocol at this level is more efficiently and more effectively to manage the risk and to be able to discharge professional care and responsibilities by working together.**

**D) Potentially Dangerous/High Risk Cases**

This would be where a professional officer, or an agency, or any person has strong concerns about an individual which requires a formal approach to other agencies who may or may not be involved in order to agree a level of risk and a joint way of managing this. If the individual has a relevant conviction the case will be dealt with through the public protection process and referred onwards to a Multi Agency Public Protection (MAPPA) meeting, as appropriate. If the individual has no relevant convictions the case will be dealt with through the Care Programme Approach. (CPA)

**The intention of the Protocol at this level is to make sure a foundation of accurate knowledge and evident can be assembled, and that this is then shared approximately to minimise risk while allowing proper management of the complex situation.**

6.3 Together these four levels form a pyramid of application – a broad base of Routine Operational Exchanges that supports and encourages when appropriate the other less frequent levels of Broad Risk Assessment and Specific Risk Management. With these in place the rare Potentially Dangerous High Risk situations will be the apex of the Protocol but will be executed when they are needed in a spirit of practiced trust and confidence between professionals and agencies.

6.4 Any agency and its employees who have significant concerns about an individual, whom they consider to present a high risk of harming someone, may use the agree MAPPA or CPA procedure, which may involve an emergency meeting. This will result in an agreement between the relevant agencies on the level of risk posed and the production of a risk management plan to reduce/manage the level of risk presented.

## **7. APPLICATION OF PROTOCOL**

7.1 It is not possible to be prescriptive about the particular procedure that staff should follow when they are concerned about the risk a person presents to the public or a potential victim. Each situation is different and should be dealt with on a case-by-case basis within the existing procedures of each individual agency. For example, not every situation of high risk is likely to be appropriate for a MAPPA meeting.

7.2 The appropriate response could be any one of the following:-

- Referral to the MAPPA (refer to MAPPA Procedures).
- A call to the Police for immediate assistance in cases of emergency
- Informing another professional of the risks that they face in a particular case.

- Undertaking a multi-agency risk assessment by contacting the Designated Officer in the Public Protection Unit of the Police to ascertain whether the MAPPA processes know the individual as a high risk (see Annex D). Or approaching another agency believed to have involvement to check out whether there is a reason to be concerned.
- Following internal agency procedures about convening a multi-agency meeting in-house, e.g. a multi-agency mental health case conference.
- Contacting the police to report a criminal activity that places members of the community at risk thereby breaching a confidence.
- Contacting another professional or professionals to plan services in the light of a person's risk thereby breaching a confidence.
- Contacting the Police to report a criminal activity that places members of the community at risk thereby breaching a confidence.
- Contacting another professional or professionals to plan services in the light of a person's risk of suicide.
- Liaising with another agency about the appropriate management of a particular individuals risk.
- Involving other agencies in a risk management plan.

## **8. MONITORING THE IMPLEMENTATION OF THE PROTOCOL**

- 8.1 Authority for this protocol and responsibility for its implementation lies with the Warwickshire Community Safety Partnership and Drug Action Team (WCSP & DAT).

The Chief Officers will ensure the protocol is adhered to and developed in the light of experience and will commission:

- Comprehensive and co-ordinated training of all relevant staff
  - Any external relations/publicity required for either promotion of the protocol or explanation of its usage in a serious incident .
- 8.2 The protocol will be reviewed every two years or earlier if major legislative changes occur.

## **ANNEX A**

### **MULTI AGENCY PUBLIC PROTECTION ARRANGEMENTS (MAPPA) PROCESS:**

#### **INTRODUCTION**

As a result of the Criminal Justice Act 2003 it has now become a statutory duty for Police, Probation and Prison Service to work with other agencies to manage the risks posed by serious offenders in their areas in a multi-agency process.

This takes the form in Warwickshire of a multi-agency process in which those cases meeting the referral criteria (see below) are subject to an initial screening procedure, and where appropriate, passed onto MAPPA. The panel will undertake a multi-agency risk assessment and, where appropriate devise a formal multi-agency risk management plan. Limited disclosure to a member of the public or another agency may be a part of this action plan.

#### **MAPPA Level 2**

Represents a lower tier panel where a multi-agency response is required, but the risks are not at the highest level. All cases that have not been screened out at an earlier stage will be discussed at level 2.

#### **MAPPA Level 3**

The Multi Agency Public Protection Panel itself represents the highest level tier of the public protection system and should be reserved for the “critical few” cases which require the most time and resources, and present the highest threats to the community with the most serious possible consequences.

#### **Role of the MAPPA**

- To assess the level of risk posed by offenders who are referred to the process by the sharing of information held by agencies
- To consider the need for, and where necessary, prepare a risk management plan
- To review the risk management plan over time
- To co-ordinate plans with Multi Agency Panels in other areas for those offender who operate across county boundaries

#### **Criteria for referral:**

The criteria for referral is set out in section 67 and 68 of the Criminal Justice and Court Services Act 2000:

- **Category 1** - All sex offenders falling within the definition of a Registered Sex Offender under the Sexual Offences Act 2003
- **Category 2** – Anyone convicted of a sex offence not included above, and anyone convicted of an offence of violence, who in either case is sentenced to 12 months

or more custody or, if found not guilty by reason of insanity, receives hospital or guardianship order since 1 April 2001

- **Category 3** – Other Offenders where; First, it must be established that the person has a conviction for an offence, which indicates that he is capable of causing serious harm to the public. Secondly, the Responsible authority must reasonably consider that the offender may cause serious harm to the public.

Not all cases falling within these criteria will be necessarily suitable for a MAPPA meeting, but will be subject to a risk assessment process within the public protection system.

### **The Threshold for Referral of Cases Falling outside Section 67 and 68 of the Criminal Justice and Court Services Act 2000 to the MAPPA:**

- That the risk presented by the subject is such that serious harm (either physical or psychological) is likely to have severe consequences for the potential victim(s) and that this harm is either imminent or very likely to occur in the near future.
- That a multi-agency approach is considered essential for the management of this risk.

NOTE: All concerns relating to a specific child or specific children should be passed directly to Children, Young Persons and Family Services under the Warwickshire Child Protection Procedures and not through the Public Protection Unit.

(All emergency situations should be passed directly through to the local Police control room for an immediate operational response)

### **Procedure for referral:**

1. The National Probation Service Warwickshire will refer those cases where an offender is sentenced to twelve months or more for a violent or sexual offence. All referrals will be on the agreed referral form, and include details of the Offender Assessment System (OASys) risk of harm category. Details of all referred cases will be circulated to nominated agency representatives, but only those cases assessed as “high” or “very high” risk will be formally discussed at the local panels UNLESS the other agency partners indicate in advance that they have information that needs to be shared.
2. The Police will refer those cases, which fall into the definition of a Registered Sex Offender.
3. Mental Health Services will refer those who by virtue or insanity receive a Hospital or Guardianship order.
4. Other agencies with significant concerns about the risk posed by an individual to the community or agencies may make a referral in the first instance by discussion with the MAPPA Co-ordinator at Police Headquarters. The MAPPA Co-ordinator will advise as to the suitability of the case for a MAPPA and suggest alternative means of dealing with the case where appropriate. Telephone 01926 415226.

## **ANNEX B**

### **VULNERABLE ADULT PROCEDURES**

Professionals who suspect that a person, who may be eligible for a service from the Children, Young Persons and Families Services, is suffering abuse should invoke the Vulnerable Adult procedures and contact the Children, Young People and Families Services.

An adult is deemed eligible for services, and therefore “vulnerable”, if they have significant difficulty in, or cannot, carry out essential life tasks and that without assistance there would be an identified risk to their life.

## **ANNEX C**

### **RISK OF HARM DISCLOSURE CHECKLIST:**

Disclosure of Personal and Sensitive Information to other agencies in Regard to the Management or Assessment of Risk:

#### **1. Remit and scope of guidance**

This guidance only applies if sharing information (that can identify someone) for the purpose of:

- Managing or assessing risk of harm where the harmful behaviour, if carried out, would be likely to constitute a criminal offence.

It should not be regarded as guidance for all other types of information exchange between the Police and other agencies about crime.

Note: Self-harm is dealt with separately in the appendix below.

#### **2. Agencies this applies to:**

This guidance only applies to the sharing of information for the above purposes with the agencies that are signatories to the Risk of Harm and Crime and Disorder Protocols.

NOTE: If the disclosure is not to one of these agencies (e.g. if it is to a Housing Association or a Voluntary Agency or a private business) then this guidance does not apply.

#### **3. Victim, third parties and witnesses:**

If the information is about a victim, is given by a witness, or by a third party, it should not be shared without the explicit consent of that individual. No agency can override this consent without compelling public protection or public interest grounds.

#### **4. Legal power to share:**

##### **With Consent:**

Any agency is able to disclose information lawfully if they have the express consent of the individual concerned to do so. This is best obtained in writing, but verbal consent can be used if it is carefully recorded.

## **Without Consent**

Clearly, for crime and risk management purposes it is not always possible or appropriate to seek an individual's consent (for example, in the case of a criminal investigation where the individual is the offender). If seeking the individual's consent would jeopardise the public protection and crime prevention or detection objectives of making the disclosure, it is likely to be inappropriate to seek it.

Where it is not appropriate to seek consent, and the purpose of the disclosure is as specified above (see 1. Remit and Scope of Guidance), you will have a power under Section 115 of the Crime and Disorder Act 1998 to make a disclosure.

The following considerations will also apply to all disclosures made without consent:

### **5. Confidentiality:**

If you owe a duty of confidentiality you can only share that information with the explicit consent of the individual unless there are strong public protection grounds for you to override that duty. Seek your own professional codes and guidance for advice about this.

### **6. Human Rights:**

Any disclosure has to be consistent with the Human Rights Act 1998, which in these circumstances usually mean Article 8 – the rights to privacy. No public body can interfere in this right unless it has reasonable grounds.

However, under the Human Rights Act 1998, reasonable grounds include the prevention and detection of crime and the protection of the health, freedoms and rights of others.

Any disclosure has to be consistent with the principle of proportionality. This means that the degree of incursion into a person's privacy has to be proportionate with the level of risk or the seriousness of the crime.

### **7. Data Protection Principles:**

Any disclosure has to be consistent with the Data Protection Principles, particularly:

- That agencies only disclose the minimum required for the purpose
- That agencies ensure that the information disclosed is accurate and relevant
- That agencies ensure that information they hold or receive is stored securely
- That agencies ensure that information received in the course of an exchange is not kept longer than is necessary
- That information disclosed has been obtained fairly

**Fairness:**

It is a requirement of the Data Protection Act 1998 that disclosures are fair. This means that if a service user/patient or witness gave information for one purpose, it should not be used for different purposes without their knowledge or consent. Agencies need to ensure that individuals giving them information are aware of the circumstances under which it might need to be shared with another agency in order for the disclosure to be fair.

**8. Warning Regarding Contentious Disclosures:**

You should be aware that if you decide to make a disclosure without an individual's consent, that individuals might try to challenge the basis on which you made that disclosure. There would be a particular risk of challenge if the disclosure you made had quite a detrimental effect on that individual's life, for example if it affected their employment prospects or their public reputation.

If you feel that a decision you are asked to make on disclosure has very serious implications, is likely to be contentious or you just are not sure about the extent to which you should make a particular disclosure without consent, you should seek legal advice. You should also be aware that if your disclosure decision was challenged you might need to justify why you thought there was a pressing need for that disclosure.

**Appendix to Disclosure Checklist (ANNEX C):**

**Self-Harm:**

Self-harm does not fall into the above guidance because it is not a criminal offence. However it may be necessary to share personal information about the risk of self-harm in order to help manage that risk under the Sharing of Information Protocol.

**With Consent:**

The best way to do this legally and ethically is with the person's consent (Health and Care Workers should refer to the Generic Protocol).

**Without Consent:**

Where consent is withheld, it will be necessary to determine the lawful basis of making this disclosure. Under Schedule 3 of the Data Protection Act 1998 any disclosure about an individual's health is defined as "sensitive information".

If an agency believes that the disclosure would be necessary for the "vital interests" of the individual (i.e. life or death), then the agency may have a lawful basis for making that disclosure. However, the decision to disclose must have regard to any duty of confidentiality and the individual's human rights.

## ANNEX D

### PROCEDURE FOR UNDERTAKING LATERAL CHECKS

1. Under Warwickshire's Sharing of Information Protocol any signatory agency may approach other signatory agencies for information if they have concerns about the risk of harm to the public or to their own staff. The purpose of approaching other signatory agencies would be to undertake a multi-agency risk assessment and share any validated concerns so the risks of harm can be managed more safely.
2. Much of the information shared under the protocol on a day-to-day basis will be between caseworkers involved with individuals who are already known to present a high risk. There are, however, occasions when an unknown individual causes concern to any agency and there is a need to find out whether such an individual is a known risk elsewhere. This guidance sets out the roles and responsibilities of agencies with regard to undertaking a multi-agency check on previously unknown individuals.
3. Where there is an immediate threat of violence to staff or to the public the agency will contact the Police immediately. The Police control room will provide an operational response to the immediate situation. (It will not provide a full lateral check based on information held on the Multi Agency Public Protection Arrangements processes).
4. Where there is the need to undertake a multi-agency risk assessment the agency with a concern must first meet the threshold of concern within its own policies before the protocol can be invoked. The cause for concern should be a concern about the likelihood of violence or other significant harm. More information may be needed to determine the level of harm accurately.
5. In most cases, for a risk assessment, the first port of call will be the Public Protection Unit. The agency's Designated Officer should make the call during office hours with an explanation of the nature of the concern. (If Designated Office is not available, the query should be made in writing). Once the Public Protection Officer is satisfied that he or she has grounds to exchange information, and has checked the identity of the caller, the following information will be provided:
  - Whether the individual is known to the Multi Agency Public Protection Arrangements (MAPPA)
  - Whether the individual is being managed through other multi-agency processes
  - Whether the individual has been known in the past and what the concerns were, if relevant
  - Which other agencies are currently or previously involved
  - Any advice in relation to maintaining public safety and/or the protection of staff

The information passed on will be the minimum required for the purpose and will be relevant and accurate.

6. It is the responsibility of the referring agency to contact other agencies that may have been involved. The referring agency will give a brief explanation of the concerns regarding the individual's risk.

All requests for information will be made through the Designated Officer of that agency. A record will be kept of the information exchange and the basis on which it was made.

7. Where there is sufficient concern following the risk assessment, the initial agency should approach the MAPPa Co-ordinator to request that the case be considered, at either a Case Conference or a MAPPa meeting.

## ANNEX E

### DETERMINING WHETHER A DISCLOSURE IS IN THE PUBLIC INTEREST:

1. The public interest is deemed for the purposes of this protocol to include:
  - Maintaining public safety/protection
  - The administration of justice
  - The apprehension of offenders
  - The prevention of crime and disorder
  - The detection of crime
  - The protection of vulnerable members of the community
  
2. In determining whether a disclosure is in the public interest and sufficient to override a duty of confidentiality the following should be considered:
  - Is the intended disclosure proportionate to the intended aim?
  - What is the vulnerability of those who are at risk?
  - What is the impact of the disclosure likely to be on the offender?
  - Is there another equally effective means of achieving the same aim?
  - Is the disclosure necessary to prevent or detect the uphold the rights and freedoms of the public?
  - Is it necessary to disclose the information to protect other vulnerable people?

## **ANNEX F**

### **YOUNG PEOPLE:**

1. Where consent is needed to share information about a young person (in law, those under the age of eighteen), it should be sought from a 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.
2. 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 understand the implications and consequences.
3. Agencies should note that they also owe a duty of confidentiality to a young person in the same circumstances that they would do for an adult (e.g. if the young person was a victim of crime).

## **ANNEX G**

### **CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 AND THE LEGAL IMPLICATIONS FOR DISCLOSURE**

This Act requires the police to record in durable form (e.g. writing, tape or computer disk) any information, which is relevant to an investigation. This information must be disclosed to the Crown Prosecution Service. The CPS does not automatically disclose “sensitive material”.

However, if the CPS considers that the information undermines the prosecution case or assists the defence case, it will either have to disclose or apply to a judge or magistrates for a ruling as to whether or not it should be disclosed. If an order is made for disclosure then either the information must be disclosed or the prosecution is dropped.

## ANNEX H

### SHARING OF INFORMATION PROTOCOL INDEMNITY:

(only to be used by non-signatory agencies)

All statutory agencies in Warwickshire are signatories to the Sharing of Information Protocol. There are situations where non-signatory agencies request information such as local crime and disorder forums. The following indemnity is intended for use by non-signatory agencies wherever necessary.

- 1 A request for information has been made by an agency/body who is not a signatory to the Sharing of Information Protocol ("the non-signatory").

.....

(Name of agency/body).

- 2 The request has been made to:

.....

(Name (s) of statutory agency) ("The Statutory Agency")

The non-signatory undertakes to comply in all respects with the provisions of the Data Protection Act 1998 and all other obligations imposed by statute and common law and will indemnify the Statutory Agency against all actions, costs, claims proceedings or demands that may be brought or made against the Statutory Agency for breach of statutory duty whether by the non-signatory, his agents or servants under the Act which arises from: -

- a) The disclosure or transfer of information for the purposes other than those specified in the Protocol
- b) The use of the information for purposes other than those specified in the Protocol
- c) Disclosure of the information to a third party
- d) Wilful misconduct or negligence in the handling, keeping or disposal of the information.

This indemnity is dated the \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_

Signed by \_\_\_\_\_

On behalf of the non-signatory.....

(Name of person and capacity in which they sign)

April 2008

# **CRIME & DISORDER PARTNERSHIP PROTOCOL**

**JOINT APPROACH TO REDUCE CRIME  
AND DISORDER AND IMPROVE  
COMMUNITY SAFETY ISSUES**

**2008**

## **CONTENTS**

### **WARWICKSHIRE CRIME, DISORDER AND ANTI-SOCIAL BEHAVIOUR**

#### **SECTION 1**

1.1 Purpose of this Protocol.

#### **SECTION 2**

- 2.1 The Protocol
- 2.2 Background
- 2.3 Procedures
- 2.4 Designated Officers
- 2.5 Personal Information
- 2.6 Extent of Personal Data Disclosed
- 2.7 Depersonalised Data
- 2.8 Non-personal Data

#### **SECTION 3**

Appendix A - Definitions

## Section 1

### 1.1 Purpose of this Protocol

1.1.1 This Protocol is an agreement between Partner Organisations specifically to facilitate and govern sharing of information relating to the prevention, detection and reduction of Crime and Disorder.

1.1.2 The purpose of this protocol is to facilitate the exchange of information in order to develop and implement the following:

- a) to comply with the statutory duty on chief police officers and local authorities under the Crime and Disorder Act 1998 to work together to develop and implement a strategy and tactics for crime reduction.
- b) under any provision of the Crime and Disorder Act
- c) helping to implement the 5 Warwickshire CDRP Crime Reduction Strategies. Links as follows:

Nuneaton & Bedworth - <http://www.nuneaton-bedworthbc.gov.uk/freedominfo/documents/504bvpp20062007.pdf>.

North Warwickshire - [http://www.northwarks.gov.uk/site/scripts/download\\_info.php?fileID=1026](http://www.northwarks.gov.uk/site/scripts/download_info.php?fileID=1026)

Rugby - [http://www.rugby.gov.uk/site/scripts/documents\\_info.php?documentID=661](http://www.rugby.gov.uk/site/scripts/documents_info.php?documentID=661)

Stratford on Avon - <http://www.stratford.gov.uk/community/community-656.cfm>

Warwick - <http://www.warwickdc.gov.uk/WDC/Community+and+living/Community+safety/default.htm>

- d) **for the purpose of tackling Anti-Social Behaviour, for example drafting an Acceptable Behaviour Contract and applying to the Magistrate's Court for an Anti-Social Behaviour Order.** The above information sharing has the legal basis of Section 115 of the Crime and Disorder Act 1998, as amended by the Police Reform Act 2002 and the Housing Act 2004 (Section 219).
- e) **information sharing between the Partner Organisations for the purpose of implementing the Government's Prolific and Other Priority Offender Strategy.** This protocol is designed to help prevent and deter, catch and convict and rehabilitate and resettle the most prolific offenders within our communities. These are all legitimate aims, which fall under the

responsibilities outlined within the Crime and Disorder Act. The above information sharing has the legal basis of Section 115 of the Crime and Disorder Act 1998, as amended by the Police Reform Act 2002.

- f) **applications for Information by a Local Authority or Housing Association, for the purposes of considering applying for a possession order in order to evict a tenant.** The application above has the legal basis of Section 84(1), Schedule 2, Ground 2 Housing Act 1985 as amended by Section 144 and 145 Housing Act 1996, and Section 152 and 153 Housing Act 1985. **Note – These Sections only give a local authority or housing association reasons for asking for information.**
  
- g) **applications for Information by a Local Authority or Housing Association, for the purposes of determining an application for persons made homeless by threat of violence or harassment.** The application above has the legal basis of Section 184 of the Housing Act 1996, in respect of Section 10 of the Homelessness Act 2002. **Note – These Sections only give a local authority or housing association reasons for asking for information.**

## Section 2

### 2.1 The Protocol

- 2.1.1 This Protocol has been written specifically for the purpose specified in section 1.1.
  
- 2.1.2 **This Protocol must be read in conjunction with the general overarching Warwickshire Sharing of Information Protocol to which the Partner Organisations have confirmed full compliance.**

### 2.2 Background

- 2.2.2 **Crime and Disorder Act 1998**
  
- 2.2.3 This protocol is recommended to the relevant authorities and those acting on their behalf), as described in the Crime and Disorder Act 1998, as the vehicle to be used in establishing clear lines of communication and procedures for the exchange of information in order to tackle root causes of crime and disorder.
  
- 2.2.4 Applications for an Anti Social Behaviour Order (ASBO) may be made to a Magistrates Court by relevant authorities, which include Local Authorities, Police and Housing Associations by virtue of the *Police*

*Reform Act 2002*. All these parties and others may also be involved in the drafting of an Acceptable Behaviour Contract (ABC). Under section 115 of the Crime and Disorder Act, Warwickshire Police and the relevant Local Authority may share information with each other and other relevant authorities so that they may make such an application. This is subject to compliance with other legislation and duties such as Human Rights, Data Protection Act etc.

2.2.5 Section 115 provides the lawful power for anyone to disclose information to a relevant authority – the police, police authority, social landlords, local authority, probation committee or health authority, or to any designated persons acting on their behalf – where this is necessary or expedient for the purposes of a provision of the Act. By virtue of the participation of the signatories to this agreement in the 5 Warwickshire CDRP's strategies for the reduction of crime and disorder, they are, for the purposes of data sharing outlined in this protocol, deemed to be persons acting on behalf of the relevant authorities in accordance with Section 115.

2.2.6 The signatories to this Protocol are persons/organisations that have been invited by the responsible authorities represented on the 5 Warwickshire CDRPs to participate in the exercise of the obligations set out in Section 6 of the Crime and Disorder Act 1998. That is to formulate and implement, for each relevant period, a strategy for the reduction of crime and disorder in the county.

2.2.7 Section 115 does not, however, override the need to disclose in a proper manner, taking into account other statutory and common law constraints on disclosure, including data protection, human rights and the common law. This Protocol puts in place sound arrangements for information sharing, so as to be clear about the process involved and the type of information to be shared to ensure compliance with data protection legislation.

## **2.2.8 Housing Act 1996**

2.2.9 This Information Sharing Protocol should comply with the requirements of Section 10 of the Homelessness Act 2002, Section 184 of the Housing Act 1996 and amendments to the Crime and Disorder Act 1998 by the Police Reform Act 2002.

## **2.2.10 Homelessness Act 2002**

2.2.11 Section 184 of the Housing Act 1996 states that Partner Organisations may make '*such enquires as are necessary*' to establish whether parties applying as homeless persons for re-housing are eligible. Section 10 of the Homelessness Act 2002, extends the 'priority groups' for re-housing to include those who have been made homeless by being the subject of violence, the threat of violence or harassment..

## **2.3 Procedures**

### **2.3.1 General Procedures**

2.3.1.2 Partner Organisations must ensure the annual Data Protection Act 1998 Notification is reviewed and completed. All relevant parties to the Protocol shall undertake to check its Registration with the Information Commissioner, to ensure that it is appropriately registered for sharing and receiving personal information for the purposes of Crime Reduction, naming the Police service as a likely recipient and source of personal data. For more details visit [www.dpr.gov.uk](http://www.dpr.gov.uk).

2.3.1.3 Where sensitive information is to be shared, explicit consent of the Individual/Guardian must be obtained **OR** reliance is put on the "protection of vital interests" justifications in Schedules 2 and 3 of the Data Protection Act 1998

### **2.3.2 Review Procedures**

2.3.2.1 The Protocol review is to be undertaken jointly by officers agreed by the Partner Organisations unless agreed by the Partner Organisation for a single Partner Organisation to undertake the review. This work will be co-ordinated by the Warwickshire Community Safety Partnership & Drug and Alcohol Team (WCSP & DAAT). At each review date the WCSP & DAAT will pull together a review group made up of DOs and identify operational problems, new legislation and highlight any proposed amendments to be agreed.

2.3.2.2 The review findings must be reported, in writing, at the next meeting of Partner Organisations or after one calendar month, whichever is the sooner.

2.3.2.3 The Partner Organisation must discuss the review, approve any resulting actions and approve an implementation plan.

2.3.2.4 Partner Organisations must agree to implement the action plan within the approved time scale.

### **2.3.3 Security Documents**

2.3.3.1 Crime and Disorder Exchanges: All requests for information exchange for a specific purpose covered by the Crime and Disorder Act 1998 will take place in writing between Designated Officers. Only DOs (Designated Officers) and PDOs (Primary Designated Officers) can

make formal requests and document agreements for the sharing of personal information. The request may be a request for information or an inter-agency or multiagency meeting.

2.3.3.2 The request will be written on agency headed notepaper (or contained within a secure email), and will set out

- What information is required
- What the purpose of the exchange is (related to the relevant crime and disorder strategy)
- On what grounds the individual's consent has been overridden (e.g. seeking consent would jeopardise the public protection, crime prevention or detection objectives of the disclosure)
- Where consent has been sought and given, the evidence of this should be provided.

2.3.3.3 The Designated Officer will log the request and make a note of the reasons for making the disclosure. Where the request is denied, the Designated Officer will also log the reasons for denying the request. The exchange will take place within ten working days (fourteen days), unless the situation is more urgent. If the situation is more urgent then the reasons for the urgency of the case will be made known and the request dealt with as quickly as practicable.

## 2.4 Designated Officers

2.4.1 In order to ensure that information is exchanged in the most efficient, effective and secure manner, the **Partner Organisations** will select and appoint **Designated Officers (DO)**. If a Partner Organisation has a Data Protection / Information Sharing Coordinator that oversees all information sharing issues, the DO will liaise with them where appropriate. DOs will assume responsibility for data protection issues; security and confidentiality; compliance with legislation; auditing and monitoring and complaints. Each Partner Organisation may put forward more than one Designated Officer for different information sharing roles. However, if it is deemed by Partner Organisations that a new distinguishable information sharing purpose has been created a new Designated Officer list for that particular purpose may be added as an Appendix to this document.

2.4.2 A person requesting information from another Partner Organisation should submit the inquiry through a Designated Officer. A reply should be made within ten working days. The request must be in writing and ideally in the relevant format. The request must be transmitted in a secure way. The source of the request will be tested periodically by the DO to ensure authentication of requestor. This may be done via a phone call to the DO. In addition it is good practice to keep a log of information shared.

## 2.5 Personal Information

### 2.5.1 Human Rights Legislation

2.5.1.1 Partners have a duty of care to share information. However, the Human Rights Act 1998 gives effect to certain Articles in the European Convention on Human Rights and requires all domestic law to read compatibly with the Convention Articles. This protocol recognises that the sharing of information has the potential to infringe a number of Convention Rights.

2.5.1.2 The Convention does allow interference of rights, known as legitimate aims.

ECHR Article 8 states that everyone has the right to respect for their private and family life, his home and his correspondence and that there shall be no interference by a public authority with his right except as in accordance with the law and is necessary in a democratic society in the interests of:

- national security
- public safety
- economic well being of the country
- the prevention of crime or disorder
- protection of public order
- the protection of health or morals
- the protection of the rights or freedoms of others.

2.5.1.3 However, the following principles should be considered:

- Is there a legal basis for the action being taken?
- Does it pursue a legitimate aim?
- Is the action taken proportionate and the least intrusive method of achieving that aim?

### 2.5.2 Data Protection

2.5.2.1 The Data Protection Act 1998 governs the way personal data are processed, regardless of format (including computerised data, CCTV images, relevant manual filing systems etc), and gives living individuals rights and protection of their information according to eight Data Protection principles.

2.5.2.2 Briefly these principles say that personal data should be:

- Processed fairly and lawfully
- Only for specified purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than necessary
- Processed in accordance with individuals rights
- Held securely

- Not transferred where there is no adequate protection

2.5.2.3 To process personal data, a justification has to be found in Schedule 2 of the Act, or in Schedule 2 and Schedule 3 in the case of sensitive data. Please refer to 2.6.6.5 for a definition.

2.5.2.4 Partner Organisations undertake that Schedule 2 of the Data Protection Act 1998 will be satisfied where it is necessary to process personal data.

2.5.2.5 Sensitive data covered by Schedule 3 should be treated with a higher degree of security and confidentiality than other personal data. Sensitive data includes information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Offences, or alleged offences
- Criminal offences / previous convictions

2.5.2.6 Partner Organisations undertake that Schedule 2 and Schedule 3 of the Data Protection Act 1998 will be satisfied where it is necessary to process sensitive data.

### **2.5.3 Crime and Disorder Act 1998**

2.5.3.1 Where the disclosure of information is necessary or expedient for the purposes of any provision of the Crime and Disorder Act 1998, Section 115 ensures all agencies have a power to disclose personal information to "relevant organisations" and those acting on their behalf. It does not impose a requirement on them to exchange information, control remains with the agency that holds the data.

2.5.3.2 For the Police in Warwickshire this might include but is not restricted to information held on the Police National Computer (PNC), or STORM.

2.5.3.3 Where it is thought necessary or expedient to exchange data to carry out the objectives of the Crime and Disorder Act 1998 a power to disclose exists in the following situations:

#### **a) Public Interest**

If consent has not been sought, or sought and withheld, the agency must consider if there is an overriding public interest of justification for the disclosure. Responsibility for considering disclosure in these

circumstances rests with the disclosing authority. In the event of doubt the **Partner Organisation** should obtain legal advice.

The rule of proportionality should be applied to ensure that a fair balance is achieved between the public interest and the rights of the data subject.

## **b) Non-disclosure Exemptions**

Personal Data can be exempt from the non-disclosure provisions of the Data Protection Act 1998. Section 29 of the Data Protection Act 1998 exempts data controllers from complying with the first data protection principle (apart from compliance with schedule 2/3) in relation to the sharing of personal/sensitive personal information. Section 29 exempts the sharer from the duty to process the data fairly (which relates largely to informing the data subject of the purposes for which the data is being shared) where doing this would be likely to prejudice:

- i. the prevention or detection of crime,
- ii. apprehension or prosecution of offenders, and compliance with the data protection principle would be likely to prejudice those objectives.

In these cases the data are exempt from the first data protection principle (but compliance with Schedules 2 and 3 continues to be necessary). Decisions must be made on a case-by-case basis. Any request for information whose purpose is the prevention or detection of crime should specify as clearly as possible how failure to disclose would prejudice this objective. The request should make clear:

- why the information is necessary, e.g. why proceedings might fail without the information;  
and
- why it is envisaged that a successful action would prevent crime, e.g. what is the projected effect of successful proceedings?
- It should be noted that Section 35 of the Data Protection Act can also provide a legal gateway.

### **2.6.1. Extent of Personal Data Disclosed**

2.6.1.1 The Designated Officer must assess on a case by case basis:

- a. why a disclosure is necessary to support action under the Crime and Disorder Act;
- b. why the public interest is of sufficient weight to override the presumption of confidentiality; and

- c. whether the information is being processed fairly and in line with the provisions of the Data Protection Act and any other relevant legislation.

The grounds upon which a disclosure is based should then be recorded on the request. This recording may not be necessary where regular information sharing is being undertaken under an existing form.

## 2.6.2 Homelessness Act 2002

2.6.2.1 Disclosure of information to the Partner Organisation will be on a case-by-case basis. The information disclosed will be **expressly** limited to:

- a. A summary of all visits to the premises as a result of relevant complaints or otherwise;
- b. A summary of any relevant incidents witnessed by Partner Organisation representatives;
- c. Details of any criminal conviction of the applicant involving relevant incidents. The offender and offences must be directly linked to reasons for the application to the relevant authority for housing or nominee. For example, if the applicant is applying for assistance for the reason of being forced into homelessness by threat of violence, any offence of violence that party has committed, or has had committed against them, may be relevant to the assessment of eligibility for re-housing.

## 2.6.3 Housing Act 1985 and 1996

2.6.3.1 Disclosure to the Partner Organisation will be on a case-by-case basis. The information disclosed will be **expressly** limited to:

- a. A summary of all relevant police visits to the premises as a result of relevant complaints or otherwise;
- b. A summary of any relevant incidents witnessed by Partner Organisation representatives;
- c. Details of any **relevant** criminal conviction of persons residing at the property.

The offender and offences *must be directly linked to the property, i.e.,* offences committed at the relevant property, or in the vicinity thereof, and care must also be taken to ensure that "spent" convictions, within the meaning of the Rehabilitation of Offenders Act, are not disclosed.

- 2.6.3.2 The Warwickshire Police's Designated Officer must ensure that any information on validated previous convictions is accurate and up to date before disclosing any such information.

## **2.7 Depersonalised Information**

- 2.7.1 The partners to this Protocol agree to share depersonalised information.
- 2.7.2 There is a requirement that information must be accurate and complete before it can be made available to other Partner Organisations. The products produced by analysing depersonalised information can be used to:
- Inform the allocation of resources to tackle crime and disorder across the County;
  - Inform any Partnership Boards/Groups/Meetings discussing Anti-Social Behaviour, Crime or Disorder and justify the final actions taken. Maps and other visual images must not be published without prior consultation with the original data owner(s).
  - No attempt must be made to identify an individual through the provision of depersonalised information;
  - Data sets must not be released to those who have a commercial interest in their use;
  - Arrangements must be made for the secure storage of all depersonalised information; and
  - Information must be destroyed when it is no longer required.

## **2.8 Non-personal data**

- 2.8.1 Signatories can use non-personalised data for crime-mapping purposes, within the remit of the Crime and Disorder Act 1998.
- 2.8.2 Partner Organisations understand that non-personalised data held 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.

## APPENDIX A

### Definitions

- a) **Personal Data:** data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of, or is likely to come into the possession of, the data controller).
- b) **Crime:** any act, default, or conduct prejudicial to the community, the commission of which, by law, renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.
- c) **Disorder:** is an expression, which refers to the level or pattern of anti-social behaviour within a particular area.
- d) **Anti-Social Behaviour:** acting in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as himself/herself.
- e) **Nuisance or Annoyance:** any conduct or other behaviour considered to be a nuisance or annoyance by a reasonable person e.g. racial harassment, sexual harassment, playing loud music, offensive drunkenness, rubbish dumping.
- f) **Relevant Authorities & those acting on their behalf:**  
Defined by section 115 of the Crime and Disorder Act 1998, for the purposes of that section  
i.e.  
a chief officer of police;  
a police authority;  
a local authority;  
a local probation board;  
a health authority.  
a chief Fire Officer

Part 6, Section 219 of the Housing Act 2004 has turned Registered Social Landlords into relevant authorities under section 115 of the Crime and Disorder Act 1998.

*Section 219 states: Disclosure of information to registered social landlords for the purposes of section 1 of the Crime and Disorder Act 1998.*

*In section 115(2) of the Crime and Disorder Act 1998 (c.37) after paragraph (d) insert – “(d.a) a person registered under section 1 of the Housing Act 1996 as a social landlord;”.*

- g) **Designated Officers:** representatives of the Partner Organisations who are the contact point for the exchange of data between such Parties and who are responsible for managing the associated administration systems.

April 2008

- h) **Prolific and Priority Offenders:** a person identified as being at risk of offending by the Prolific and Priority Offender Steering Board made up of Partner Organisations.

April 2008

April 2008