# COMMUNITY SAFETY INFORMATION SHARING PROTOCOL

## JOINT APPROACH TO MAKE WARWICKSHIRE A PLACE WHERE PEOPLE FEEL SAFE TO LIVE, WORK AND VISIT

COMMISSIONED BY THE SAFER WARWICKSHIRE PARTNERSHIP BOARD

December 2013

# Index

# 1 Introduction

1.1 The Safer Warwickshire Partnership Board is responsible for putting in place an information sharing protocol to facilitate information sharing between responsible authorities for community safety in Warwickshire.
This should be agreed, by all responsible authorities, statutory agencies and other groups, providing community safety.

1.2 The purpose of this information sharing protocol is to facilitate the secure sharing of information between partner agencies in Warwickshire, govern the secure use and management of information and enable agencies to meet their legislative obligations effectively under Section 17 of the Crime and Disorder Act 1998 (as amended by the Police and Justice Act 2006 and the Policing and Crime Act 2009).

1.3 This information sharing protocol provides specific details for information sharing within a community safety context. It is a tier 2 agreement and should be read in conjunction with the tier 1 Warwickshire Information Sharing Charter, which sets the standards for obtaining, recording, holding, using and sharing information

1.4 This protocol will remove the need to produce other tier 2 protocols covering all aspects of community safety in Warwickshire.

1.5 However, as well as this generic information sharing protocol a number of more specific tier 2 protocols have been developed for specialist service areas where legislation requires more prescriptive data sharing guidance or different partners are involved, e.g. Multi Agency Public Protection Arrangements (MAPPA). These additional protocols are designed to work alongside this one.

# 2 Purpose of Information Sharing

2.1 The purpose of this Protocol is to facilitate the exchange of Information, other than depersonalised information, in order to comply with the statutory duty placed on the responsible authorities (Local Authorities, Police, Fire and Rescue Authority, Health and Probation) to work together to develop and implement a strategy and tactics for reducing crime and disorder, anti social behaviour and substance misuse. This will also include when an individual poses a risk of harm to the community, specific potential victims or professionals and any other behaviour affecting the local environment.

2.2 This Protocol will also extend to co-operating organisations and any other agency or organisation, which is a signatory to this Protocol.

2.3 Information sharing is the cornerstone of delivering shared understanding of issues and arriving at holistic solutions. Effective delivery relies on good decision making and those decisions should be based on good information. The right information enables partners to carry out evidence-based, targeted community safety interventions and enables them to evaluate their impact. The improved outcomes of an intelligence led, problem solving approach to community safety can only be achieved when partners have access to relevant, robust and up-to-date information from a broad range of sources.

2.4 Partners should also consider the likely effect of not sharing information, for example, harm to individuals, damage to their organisations' reputation, a disconnect in partnership working and lack of understanding of problems.

2.5 Much of this information will be depersonalised data, but it is also necessary to share personal information, notably where decisions about particular individuals or families are being made. Bringing resources together through responsible information sharing reveals a more accurate picture of what is going on in a local area. This improves analysis, decision making and better informs resource allocation.

# 3 Who will be sharing information?

3.1 Partners who are required to share information are named as the responsible authorities in the 1998 Crime and Disorder Act, as amended in the 2006 Police and Justice Act and 2009 Policing and Crime Act. These are the Police, all Local Authorities, Fire and Rescue Service, Clinical Commissioning Groups and Probation Trust.

3.2 Co-operating bodies under the Act may be asked to share information. These are the Parish Councils, School & College Governing bodies, Registered Social Landlords and agencies appropriate to the location or circumstances.

3.3 Various other bodies are named as invited participants under the Act and may also be asked to share data for crime and disorder purposes.

3.4 Reasonable attempts should be made to ensure that voluntary organisations participating in information sharing in accord with this agreement have all their information sharing policies in place.

# 4 What is to be shared?

4.1 The 'Delivering Safer Communities' guidance and the Crime and Disorder (Formulation and implementation of Strategy) Regulations 2007 requires the statutory agencies of the Community Safety Partnerships to share information.

4.2 Shared information will usually include a location reference, information about the nature of the problem, and, where relevant, names and addresses of offenders, victims or witnesses.

4.3 Some of this information will be sensitive as defined by the Data Protection Act 1998. However, sharing of this type of sensitive information is allowed in appropriate circumstances under legislation including the Crime & disorder Act 1998, Criminal Justice Act 2003 and Statutory Instrument 1831.

4.4 In order to share appropriate information between partners there must be a lawful, defined and justifiable purpose(s) which supports the effective delivery of a policy or service that respect people's expectations about the privacy and confidentiality of their personal information but also considers the consequences of a failure to act. This agreement is supplemented by a number of questions, included at Appendix 1, designed to 'walk' Managers/Designated Persons and other specialist support through a process to assess the impact and appropriateness of information sharing.

4.5 'Signatories' to this Protocol understand that personal data will principally be shared at multi-agency meetings (see Section 6). However there will be other ad hoc arrangements for sharing information. For example there may be meetings between members of staff from different agencies sharing information about a common case in order to build a foundation of accurate knowledge and evidence, to minimise the risk of harm to the community, whilst allowing proper management of the case. As well as meetings the Protocol covers other forms of information exchange, such as ECINS. The intention of this Protocol is to cover all such information sharing provided the safeguards described in the Protocol are followed.

4.6 If any personal data relates to an ongoing investigation or prosecution by any of the agencies then consultation must take place with the investigating officer and Crown Prosecution Service as the matter will be sub-judice. This will ensure that disclosure will not adversely prejudice the outcome of the matter.

# 5. Fairness and Transparency

5.1 Partner organisations must take reasonable steps to tell service users what type of information about them may be shared, who it may be shared with, and the likely consequences of sharing. If the service user agrees to this sharing, they will have given informed consent. This should be recorded.

5.2 If the information is considered confidential or restricted (see 6.4) and the service user does not consent to sharing, it can only be shared following a risk assessment which considers the impact of not sharing on a service user's welfare, or a court order or statute require or permit sharing without consent. Where consent is withheld or withdrawn the guidance emphasised how decisions may be made about sharing information through specific legal powers and application of principles such as proportionality. The question listed at Appendix 1 will help to assess the impact of service users of decisions relating to information sharing.

5.3 The Data Protection Act 1998 allows for disclosure where it would be in the public interest but when consent has not been sought or has been withheld. This includes:

Prevention of crime including
Prevention of disorder
Protection of public safety
Protection of rights and freedoms of all
Protection of children, young people and vulnerable adults.

5.4 If informed consent has not been sought or sought and withheld, the agency must consider the public interest to justify disclosure. This consideration must identify a condition for processing in accordance with Schedule 2 of the Data Protection Act 1998 and Schedule 3 if appropriate. A key factor in deciding whether or not to disclose information is proportionality i.e. is the proposed disclosure a proportionate response to the need to protect the potential victim? The amount of information disclosed and the number of people to whom it is disclosed should be no more than is necessary.

# 6. Arrangement for Data sharing within Multi-Agency Meetings excluding MAPPA

6.1 Using the definitions in 6.4 of this agreement the chair should designate the level of confidentiality appropriate to the information being shared at the outset and, where relevant, provide a signing-in sheet (Appendix 2) which states the data handling and sharing requirements relevant to the designation. If used the chair should retain a copy of this signing-in sheet.

6.2 The parties to this Protocol understand that in keeping with government initiatives to invite a wider spectrum of society to assist the relevant authorities to implement the Crime and Disorder Act 1998, it is likely that there will be individuals present at certain meetings who are not representing an organisation which is a signatory to this Protocol. To allow for this, the signing-in sheet should state that the signatory agrees to abide by all the terms of this Protocol (see Appendix 2).

6.3 It is good practice to use the Government protective marking scheme. This sets out levels of confidentiality and appropriate security measures. 'Protective Marking' is the method by which the originator of an asset (that is all material assets, i.e. papers, drawings, images, disks and all forms of electronic data records), indicates to others, the levels of protection required when handling the asset in question, in terms of its sensitivity, security, storage, movement both within the guidance and outside the originator's own department or force and its ultimate method of disposal.

6.4 The levels of restriction are:

Confidential - The effects of releasing information marked as *Confidential* include considerable infringement on personal liberties, material damage to diplomatic relations, or to seriously disrupt day-to-day life in the country.

.

Restricted – Information marked as *Restricted* is at a level where the release of the material will have effects such as significant distress to individuals, adversely affecting the effectiveness of military operations, or to compromise law enforcement

Protect - Such information will cause distress to individuals, cause financial loss or improper gain, prejudice the investigation or facilitate the commission of a crime or disadvantage government in commercial or policy negotiations with others.

# 7. Process for data sharing outside meetings

7.1 This agreement has been formulated to facilitate the exchange of information between partners. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of each case.

7.2 Partners' sharing information should make clear who the information can be shared with, information shared should only be used for the purpose requested and should not be shared further without consent of the information owner.

7.3 Any data should be shared and stored in accordance with the relevant legislation. In particular where the data to be shared is personal, a secure transmission system should be used, such as secure email or courier or hosted on a secure system shared by partners. (Appendix 3)
Tier 3 operating procedures should be agreed for each purpose.

7.4 Any information shared should only be kept as long as it is necessary and then confidentially destroyed by all signatories.

7.5 Appendix 1 gives a checklist to help ensure that data is lawfully shared.

# 8. Nominated representatives

8.1 Each Partner Organisation shall have a Designated Officer who will facilitate data sharing where issues arise.

8.2 Any disputes or disagreements between parties, including why one agency decides not to share information with another, shall be resolved by discussion between the Designated Officers, if at all possible, or between the heads of each agency.

# 9. Data Controller Responsibilities

Data Controllers must make appropriate notification to the Information Commissioner as defined by the Data Protection Act 1998 and the Information Commissioner.

# 10. Agents and Sub-contractors

Each Partner Organisation shall ensure its agents and sub-contractors comply with the provisions of the Protocol.

# 11. Complaints

11.1 Each Partner Organisation will deal with the complaints in accordance with their own procedures, which will ensure that:

Service users are aware that they can complain and of how to go about it.
Complains are acknowledged promptly in writing
The complaint is investigated fairly and thoroughly;
Service-users are given an appropriate written response;
If appropriate the appeals procedures are explained to the service-user.

11.2 If two or more Partner Organisations receive a complaint about the same matters, they should investigate and respond to the complaint jointly.

11.3 If a Partner Organisation receiving a complaint believes another Partner Organisation may be responsible, wholly or partly, for the matters complained of, it should notify the other organisation and the organisations should investigate and respond to the complaint jointly.

# 12. Non compliance and Partner Disagreement

12.1 In the event of a suspected failure within their organisation to comply with this Agreement, Partner Organisations will ensure that an adequate investigation is carried out and recorded. If the Partner Organisation finds there has been a failure it will ensure that:

Necessary remedial action is taken promptly;
Service-users affected by the failure are notified of it, the likely consequences, and any remedial action.
Partner Organisations affected by the failure are notified of it, the likely consequences, and any remedial action

12.2 If one Partner Organisation believes another has failed to comply with this Agreement it should notify the other Partner Organisation in writing giving full details. The other Partner Organisation should then investigate the alleged failure. If it finds there was a failure, it should take the steps set out above. If it finds there was no failure it should notify the first Partner Organisation in writing giving its reasons.

12.3 Where it is clear that a partner organisation is not complying with this Protocol, other Partners may decide to stop sharing information until the issues are resolved.

12.4 More information about information sharing is available from the Information Commissioner. Go to: http;//www.ico.gov.uk/

12.5 Partner Organisations will make every effort to resolve disagreements between them about personal information use and sharing. However, they recognise that ultimately each organisation must exercise its own discretion in interpreting and applying this Agreement.

12.6 Nominated representatives should ensure they are notified at an early stage of any suspected or alleged failures in compliance or partner disagreements relating to their Partner Organisation.

# 13. Retention and Disposal

Partners must comply with their own agencies retention and disposal policies.

# 14. Access to Information

Partners must have in place policies to deal with people's right to access under Freedom of Information (FIO) or Data Protection Act (DPA)

# 15. Monitoring and Review

The Safer Warwickshire Partnership Board will monitor and review the contents and implementation of this Information Sharing Agreement. The review will have regard to

Changes in the relevant law and statutory or other government or national guidance:
Service-user and staff opinions, concerns and complaints:
Failures in Compliance and disagreements between Partner Organisations;
Any other relevant information.

# 16. Change History

| Version | Amended by | Amended date | Summary of main changes |
|---|---|---|---|
| | | | |
| | | | |

# 17. Effective Date

This Protocol is effective from an agreed common implementation date 18 December 2013 and will be subject to a common review period 24 months from the implementation date.

# Appendix 1 – Do we need this information?

1. Why do I want the information? Is sharing this information in the best interests of the victim or offender?

2. Is there a sufficient need to know? If the information is shared will this make a difference to the service offered and to the outcomes for the victim or offender? Is it necessary for me to do my job or to fulfil a statutory duty?

3. Is the reasons for the request "proportionate" for the purpose e.g.

    - Are the reason or reasons for sharing information justifiable under Article 8 of the Human Rights Act?
    - Can less information be shared and still achieve the best interest of the victim/offender?
    - Is there another equally effective way of achieving the same aim? Can I share less information and still achieve the best interest of the victim/offender.
    - What is the impact of disclosure likely to be on the individual?
    - If the information requested is sensitive information (race or ethnicity, political or religious beliefs, health, sexual life, criminal offences, trade union membership), is it necessary to share this in order to meet the reason for sharing?

4. Is the information up to date and accurate? (Care should be taken when recording the name, date of birth and address to ensure that when data is merged from different agencies it relates to the same person).
   Also do I distinguish between fact and opinion or judgement?

5. Will the request involve secondary disclosure and if so do I need to check with the person who told me this information or wrote this report before I share it?

6. Have I got consent? If so is it recorded on a file or is there a consent form, are here any restrictions?

7. On the assumption that the consent cannot realistically be obtained or sought is there justification for sharing without consent, e.g. to protect the interests of the victim/offender?

8. Have I recorded that I have shared this information?

9. Am I sharing this information in a secure way?

Name of Meeting _____

Date of Meeting _____

Location of Meeting _____

# Appendix 2 – Restriction level – Protect/Restricted/Confidential

Please note, by signing this sheet you are agreeing to comply with the relevant handling rules for protective marking (Appendix 3) and the requirements of the Safer Warwickshire Partnership Board Community Safety Information Sharing Agreement and/or the specific Information Sharing Protocol applicable to this meeting.

Information shared should only be used for the purpose requested and should not be shared further without consent of the information owner.

| Name | Signature | Representing |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Please delete as appropriate. Protect – data to be shared may cause distress to individuals. Restricted – date to be shared is personal data about an offender, victim, or witness. Confidential – data to be shared is personal and of a sensitive nature.

# Appendix 3 – Current Handling rules regarding protectively marking material

**(to be reviewed in 2014)**

| **Your Action** | **Restricted** | **Confidential** |
|---|---|---|
| Marking | Top and Bottom of each page | Top and bottom of each page |
| Storage of papers | Protected by one barrier for example a locked container | Protected by two barriers. e.g. a locked container in a locked room within a secure building |
| Disposal of papers, inc photographs | Downgrade by tearing into small pieces and place in secure waste sacks or use a cross cut shredder. Keep secure when unattended | Downgrade by tearing into small pieces and place in secure waste sacks or use a cross cut shredder. Keep secure when unattended |
| Disposal of magnetic media | Securely destroy. CD Roms – destroy completely – disintegrate, pulverise, melt or shred. | Securely destroy. CD Roms – destroy completely –Disintegrate, pulverise, melt or shred. |
| Movement between partner agencies | By post or courier, in a sealed envelope. Do not show protective marking on the envelope. | By post or courier, in a sealed envelope. Double enveloped and both fully addressed. Protective marking shown on inner envelope only. Return address on outer envelope. |
| Public telephone network/Mobile Telephone, inc text messages | May be used. Digital mobile phones may be used. For analogue mobile phones. Use guarded speech and keep conversation brief | Only if operationally urgent. Use guarded speech, and keep conversation brief. Do not use analogue mobile phones |
| E-mail | Only to be used when sent to secure networks e.g. pnn. gsi. gsx etc | Not to be used unless encrypted |
| Internet | Government approved encryption required | Not to be used |