

## Welcome Page

Welcome to the “Model” Protocol section, on the Crime Reduction Website.

The Crime & Disorder Act 1998, laid the foundations for a joined-up approach to tackling Crime and Disorder, by establishing local partnerships between local authorities and police forces, together with various other bodies invited to co-operate [See Appendix for detail]. The act gives these partnerships a legal power to share information, for the purpose of preventing or reducing crime and disorder under an agreed objective.

All Protocols are agreements of no legal standing between various parties. They are drawn-up for the specific purpose of clarifying the process and types of information that may be exchanged. They should always be presented in as plain English as possible.

Protocols are “living” documents. As such, they are always susceptible to the changes in law and best practice, and should be updated and amended regularly. **The sharing of information is not something to be afraid of, and it is fundamental to the success of any strategy to reduce crime and disorder.** There is a decision making process that can be associated with all disclosures, and this “Model” protocol will assist designated officers to identify the relevant issues. It also aims to encourage a significant level of standardisation in the information exchange by partnerships.

The Contents page, sets out all the relevant sections of the “Model” Protocol. **You must work through all the sections in order, to ensure that you have covered all the sections of the “Model” Protocol relevant to your data sharing arrangements.**

The model is a guideline and may not cover every type of information sharing arrangement by crime and disorder partnerships. It is intended as a best practice way to approach a data sharing agreement; you can tailor it to your needs.

**You need to select those clauses which best fit your frame of work, and fill-in your details wherever indicated. The Appendix section contains full details on legal and procedural aspects.**

**Guidance about using this protocol is written in blue, while the actual text of the “Model” Protocol is written in black.** Wherever you see the blue text, you should select the drop-down box range of options (which will

always include a free text line), and insert your details, if your option is not available. The computer will remember all text selected and at the end of the process, you will be able to print out a final, personalised version of your Protocol.

We have included a **Library section on good Information Sharing Protocols** [\[subject to approval\]](#), for your perusal. This is so you can have a look at some of the Protocols that are currently in use.

**NB: Indemnity Clause;** As Protocols are not legally-binding documents, it is wrong to assume that mention of these Indemnity Clauses in any Protocol would place all signatories beyond legal challenge, following a breach or disclosure of certain sensitive information. We have thus omitted an Indemnity Clause from our “Model” Protocol, but it may be an option for your organisation.

## CONTENTS SECTION

- 1) Title Page
- 2) General Introduction
- 3) Golden Rules & Undertaking
  
- 4) Non-personal Data
- 5) Depersonalised Data
- 6) Personal Data
- 7) Sensitive Data
  
- 8) Designated Officers
- 9) Process of Information exchange
  
- 10) Security and Data Management
- 11) Complaints and Breaches
- 12) Audit
  
- 13) Signatories page
- 14) Glossary to the Protocol
- 15) Appendix section

TITLE SECTION

**“THE [Insert group name of  
Partnership] PROTOCOL  
AND PROCEDURE FOR  
THE EXCHANGE OF  
[Specify here]  
INFORMATION, AS  
AGREED BETWEEN  
[Insert name of parties here]”**

[Insert Table 1, to illustrate the types of bodies required to participate, required to co-operate, and invited to participate in the Protocol, as part of the Crime Reduction Partnership Strategy, set-out by the Crime and Disorder Act 1998].

[Insert the most current review date here, at foot of page]

## INTRODUCTION SECTION

- 1) **Purpose:** The purpose of this Protocol is to facilitate the exchange of information pursuant to the power contained in Section 115 of the Crime and Disorder Act 1998. Where certain conditions are satisfied, Section 115 enables any person to disclose information for the purposes of any provision of the Crime and Disorder Act 1998 to a relevant authority [see glossary], or to a person acting on behalf of such an authority.
  
- 2) Relevant provisions of the Crime and Disorder Act 1998, include;
 

[\[insert as many provisions as on list in appendix\]](#).
  
- 3) **The Crime & Disorder Act 1998** is the primary legislative tool, common to all crime reduction Protocols. It does not override existing legal safeguards on personal information. [\[See appendix for descriptions of relevant sections from all legislation, including below\]](#).
  
- 4) By signing this protocol, we declare our commitment to the procedures it sets out. The manner in which information can be exchanged takes into account the following legislation;
  - a) **The Data Protection Act 1998**, for the processing of personal information
  - b) **The Human Rights Act 1998**, for the rights of the individual's privacy
  
- 5) The following legislation will also be relevant to us. [\[Please select those that will need to be added to your Protocol\]](#);
  - a) **Common Law Duty of Confidence** [\[social services, medical profession patient confidentiality, police\]](#)
  - b) **The Freedom of Information Act 2000**
  - c) **The Housing Act 1996** [\[for RSLs\]](#)
  - d) **The Mental Health Act 1983** [\[for health sector\]](#)
  - e) **Health & Social Care Act 2001** [\[for health/social services\]](#)
  - f) **Education Act 1996**
  - g) **Children Act 1989**
  - h) **NHS and Community Care Act 1990**
  - i) **Sex Offenders Act 1997**
  - j) **Any other relevant Legislation.** [\[eg section 37 & 39 of CDA, for YJS\]](#)
  
- 6) The scope of this Protocol is to clarify as far as is possible, under which circumstances information can be exchanged. The intention is that a

single, joint approach to exchanging information, is a highly efficient mechanism for reducing crime and disorder.

- 7) It is the purpose of this Protocol, to clarify the understanding between [insert names of parties], on each party's responsibilities and duties towards each other. We are fully aware of the process for information exchange and will comply with all legal requirements.
- 8) All technical terms and abbreviations, are defined in the extensive Glossary section. Descriptions of all relevant legislation and other material, are set-out in detail in the Appendix.
- 9) [Where possible,] This Protocol should be published and made available to the general public, for clarity of purpose.
- 10) This Protocol is due to be next reviewed on [insert date], and any comments should be sent to [insert name of PDO and address.]
- 11) Any partner may withdraw from this Protocol upon giving written notice to the other signatories. Data which is no longer relevant should be destroyed or returned. The partner must continue to comply with the terms of this Protocol in respect of any data that the partner has obtained through being a signatory.
- 12) ["Health Warning"]- We agree no exchange of information especially personal information, should take place until each and every party to the exchange has signed up to this Protocol.

## “GOLDEN RULES” SECTION

- 1) As parties signed-up to this Protocol, we recognise the importance of sharing information with each-other, in line with the aims of the Crime and Disorder Act 1998, for the purpose of reducing crime and disorder.
- 2) Parties in this Protocol undertake to co-operate fully with each-other, within the parameters of the Data Protection Act 1998, the Human Rights Act 1998 and the Crime and Disorder Act 1998, and in accordance with the Home Office guidance associated with these Acts. [\[Add other relevant legislation to your Protocol here\]](#).
- 3) We pledge to periodically [\[to be agreed between partners here\]](#), consult with each-other upon matters of policy and strategy.
- 4) We undertake in this Protocol that where possible and appropriate, information requested in the correct manner ([see process section](#)), is given within a time limit of [\[to be agreed\]](#) days; this may vary depending on the nature, volume of requests and operational need.
- 5) Each partner pledges that all personal data remains the property of the disclosing agency, and is the responsibility of the data controller as defined by the Data Protection Act 1998. [\[Insert names of PDO and DO's\]](#). The partner receiving the data will not normally use it for any purpose other than that set-out in this Protocol, nor share it with any other party, without the disclosing partner's written permission.
- 6) Each [\[insert names\]](#) party undertakes to ensure that it complies with all relevant legislation, this Protocol, and its internal policies on **disclosure**. Parties are recommended to seek their own legal advice, wherever necessary.
- 7) We agree to disclose information to [\[insert names of parties\]](#) who are relevant authorities or who are acting on behalf of a relevant authority for the purposes of the Crime and Disorder Act 1998. Where the recipient is acting on behalf of a relevant authority, this means in their capacity as persons selected by the relevant authority to formulate or implement the crime and disorder strategy.

NB: Education establishments carrying out research and analysis on behalf of the partner members and evaluation and monitoring of initiatives, ie burglary reduction.

- Further disclosure of the same data to persons/agencies outside this Protocol would be regarded as “Secondary Disclosure” and would not normally be allowed, unless that body was brought into this information-sharing Protocol, in the proper manner. [Insert Table 2 on guidance for sharing information].

8) The information disclosures will consist of;

[Insert list of Information types here. List as many as you require from tables 3& 4 in appendix.]

[After you have listed information types, you must qualify your chosen types in free text here.]

9) [Insert names] Each party pledges to check its data notification to ensure that it is appropriately registered for sharing and receiving personal information for the purpose of crime reduction. Each party also pledges to ensure that the data it holds is as accurate and up to date as possible.

10) We agree when **handling the Media,**

- a) to be fair to our fellow partners, and maintain their integrity
- b) when providing information to the public, to do so honestly and fairly
- c) statements must reflect the multi-agency decision process
- d) consent of the data owner will be sought prior to release to the media
- e) where practical, individual data subjects will be consulted if the media coverage was such that it may identify the individual. [Circumstances may exist that make this impractical, such as where the current whereabouts of the data subject is unknown, or the purpose of the media coverage is to identify the individual data subject.]

## NON-PERSONAL DATA SECTION

[\(Select this or skip to next section\).](#)

- 1) We understand that non-personal data constitutes data that has never referred to individuals. Non-personal data is more often than not aggregate data. [\[see glossary\]](#). It is non-personal data (never has referred to an individual) or aggregated data (derived from personal, non-personal and de-personal data), that is normally used for crime-mapping. We can use this non-personal data for crime-mapping purposes, within the remit of the Crime & Disorder Act 1998.
- 2) We agree that non-personal information held by us may be subject to the provisions of the Freedom of Information act 2000. We have the legal duty to provide non-personal data to a third party, if a formal request is made.
- 3) We will disclose non-personal data for the purpose of profiling local areas for crime activity, and to calculate the cost, scope and scale of proposed crime reduction interventions by our partnership.

## DEPERSONALISED DATA SECTION

[\[Select this or skip to next section\]](#)

[This type of data is seen as a good method for exchanging the information required, as long as this can achieve the required objective]

- 1) We accept that depersonalised data is used in the vast majority of Crime Audit activity, as management teams and consultants do not require personal data. Depersonalised data is excellent for profiling local areas, and in calculating the scale, scope and cost of proposed crime reduction interventions.
- 2) We understand that depersonalised data encompasses any information that does not and cannot be used to establish the identity of a living individual, and has had all personal identifiers removed. We note that the Information Commission has stated that even a post-code or address can give away the identity of an individual, if there is only one person living there.
- 3) We accept there are no legal restrictions on the exchange within this Protocol of depersonalised data, although a duty of confidence may apply in certain situations, or a copyright, contractual or other legal restriction may prevent the information being disclosed to partners.
- 4) We appreciate that if several sets of depersonalised data were merged or compared to each-other, there is a risk that an individual could be identified. We will always hold depersonalised data securely and destroy it securely, when no longer required.
- 5) It is good practice where possible to give subjects information about how anonymised data about them may be used (particularly for sample healthcare patients.)

## **PERSONAL DATA SECTION**

### **(Select or skip to next section)**

- 1) We understand that personal data is information which relates to a living individual who can be identified from the data; this data will be clearly marked as personal data and kept securely within a pass-worded computer system or otherwise physically secure with appropriate levels of staff access. We undertake to destroy all personal information when no longer required for the purpose for which it was provided.
- 2) We undertake to formally record all grounds for disclosure of personal information. We will process information fairly and objectively for each case. We agree that we will only disclose sufficient information to enable our partners to carry out the relevant purpose for which the data is intended. This we will determine on a case by case basis.
- 3) Personal information should only be shared in a particular case when we, as the disclosing partner, are satisfied that; a) We are legally empowered to do so. The conditions of schedule 2 of the Data Protection Act 1998 must be satisfied [\[see appendix\]](#). b) The proposed disclosure of personal information can be done in accordance with the principles of the Data Protection Act 1998. c) We can disclose personal information reflecting the common law of confidentiality and the principles of the Human Rights Act 1998.
- 4) Section 115 of the Crime and Disorder Act 1998 provides us with lawful power for disclosure where this is for the purpose of implementing the provisions of the Act. However, although the Act creates a situation where the disclosure of information may be lawful, the presumption of confidentiality will still apply.
- 5) We will only disclose personal data relating to a victim, informant or witness with the consent of the data subject, (unless there is an overriding public interest in disclosure). This will be to [\[name\]](#) staff or posts to enable them to carry out their duties in the exercise of a public function. Medical practitioners who are bound to be registered with the General Medical Council are expected to take into account the guidance of confidentiality by the latter. [\[See appendix for guidance.\]](#)

-We can also disclose on a case by case basis, for the following reasons (provided there is a lawful basis for disclosure, where there is a substantial chance that one of the following purposes would be prejudiced);

- a) to prevent or detect crime
  - b) To apprehend or prosecute offenders
  - c) If it is required by law (bulk disclosures are also normally allowed)[see [glossary](#)]
  - d) If the disclosure is registered with the Information Commissioner.
- 6) When disclosure is required, we agree to ensure that;
- a) the information is being processed lawfully: the information is being processed fairly
  - b) the public interest is of sufficient weight to over-ride the presumption of confidentiality and to justify any interference with the right to privacy etc in Article 8 of the European Convention of Human Rights
  - c) a disclosure is necessary to support action under the Crime and Disorder Act
  - d) any disclosure must have regard to specific statutory restrictions on disclosure.
- 7) We understand the Public Interest criteria, to include;
- a) the administration of justice
  - b) maintaining public safety
  - c) the apprehension of offenders
  - d) the prevention of crime and disorder
  - e) the detection of crime
  - f) the protection of vulnerable members of the community.
- 8) **NON-DISCLOSURE EXEMPTIONS:** We agree any request for information by a partner must specify as clearly as possible, how failure to disclose the information would jeopardise the crime reduction objective, as set-out in s29(3) of the Data Protection Act 1998. It must be stated why the case might fail without this information, and what the assumed effect of the successful case might be, following successful disclosure.
- 9) **HUMAN RIGHTS ACT 1998:** Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, 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 and is necessary in a democratic society in the interests of;

- a) National Security
- b) Public Safety
- c) Economic well being of the country
- d) The prevention of crime and disorder
- e) The protection of health or morals
- f) The protection of the rights or freedoms of others.

10) **PROPORTIONALITY:** If the disclosure of information will in some way restrict the rights of the data subject, we will consider the rule of proportionality. This is to ensure that a fair balance must be achieved between the protection of the individual's rights, with the general interests of society.

11) **CONFIDENTIALITY:** We undertake that information will only be used for the purpose for which it was requested, and will securely store it and destroy it when no longer required. We understand that outside agencies wishing to be part of the information sharing process, will upon signing this protocol, be bound to comply with its terms.

12) **[Include if appropriate or skip to 13].**

**CAUTIONS & CONVICTIONS:** We agree that details of cautions (or reprimands/ warnings issued under the Crime and Disorder Act) which relate to an adult will not generally be disclosed as the cautioning procedure creates an expectation that the offence has been dealt with and that no further action will be taken. Normally, the only exception will be the vetting of applicants for unitary authority and health authority/trust posts that involve contact with children and young persons, where the vetting is part of implementing a strategy for the reduction of crime and disorder pursuant to section 6 of the Crime and Disorder act 1998.

We understand that the exchange of personal information post conviction will be subject to the same presumption of confidentiality. However, the prevention of crime and administration of justice, as provided for in the Crime and Disorder Act 1998, are obviously in the public interest and may provide the grounds upon which a disclosure can be justified.

Details of convictions recorded on the Police National Computer, or retained on file by us, can be released to another designated officer where this is justified in the public interest, to support proceedings under the Crime and Disorder Act 1998. We recognise that we must exercise

care in the disclosure of conviction data and a designated officer must ensure that information is accurate and relevant to an enquiry before it is released.

### 13) [Include if appropriate.]

**YOUTH OFFENDING TEAMS:** It is permissible for information to be disclosed to the members of a youth offending team (or local youth justice team) for the purpose of any provision of the Crime and Disorder Act 1998.

Following the initial referral, designated officers attached to the team will be responsible for the further disclosure of relevant personal information and conviction data.

There may be occasions when it is necessary for members of the youth offending team to disclose personal information to another agency. In such circumstances the following guidelines must be followed;

- a) A secondary disclosure of personal information must generally be authorised by the original data owner.
- b) The disclosure must support action under the Crime and Disorder Act 1998.
- c) The public interest must outweigh any duty of confidentiality and must justify any interference with the right to privacy under Article 8 of the European Convention of Human Rights 1998.
- d) The information must be processed fairly.

The youth offending team manager will be responsible for ensuring that personal information provided to the team is stored in a secure place and destroyed when it is no longer required.

## SENSITIVE DATA SECTION

[\(Select this or skip to next section\)](#)

- 1) We must always consider whether we are processing sensitive personal data, which is data that falls into the following categories;
  - a) racial or ethnic origin
  - b) sexual preference
  - c) physical or mental health
  - d) membership of a trade union
  - e) political or religious beliefs
  - f) criminal offences and proceedings
- 2) We undertake that where we process the above sensitive data, we will need to satisfy schedule 2 and schedule 3 of the Data Protection Act 1998. [\[See appendix for schedules.\]](#)
- 3) **CONSENT:** Where appropriate and possible, explicit consent should be obtained from the data subject for the disclosure to take place, in accordance with the Data Protection Act 1998. This consent must be freely given, after the consequences are made clear to the person from whom permission is being sought. [\[See glossary for definitions of consent.\]](#)
- 4) **For our purposes, we may process sensitive information lawfully using section 115 of the Crime and Disorder Act 1998. However, we need to be aware of other legal obligations such as the common law duty of confidence.**
- 5) If we must disclose sensitive data held under a duty of confidence, we will consider whether we can obtain the data subject's consent. If we cannot, then we must consider the grounds on which we can over-ride the consent issue. We will still be able to disclose sensitive information if this is in the defined category of **public interest**.

**PUBLIC INTEREST:** We must decide after consent has been refused or withheld, if there is an over-riding public interest to justify the disclosure. We agree to consider the following;

- a) Is the intended disclosure proportionate to the intended aim?
- b) What is the vulnerability of those who are at risk?

- c) What is the impact of disclosure likely to be on the offender?
  - d) Is there another equally effective means of achieving the same aim?
  - e) Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
  - f) Is it necessary to disclose the information, to protect other vulnerable people?
- 6) Any disclosure of sensitive information by the partner, should be restricted to the minimum necessary to achieve the purpose and be as generalised as possible.

## DESIGNATED OFFICERS SECTION

- 1) We understand that each partner must appoint a Primary Designated Officer (PDO see glossary), who will be a Manager of sufficient standing, and have a co-ordinating and authorising role. We may also appoint further Designated Officers (DO's) within the same body; these staff names are listed in the appendix.
- 2) The following named individuals are designated to assume responsibility for data protection (including notification where appropriate), security and confidentiality, and compliance with all relevant legislation;

<b>NAME</b>	<b>POST</b>	<b>ORGANISATION</b>
[Insert name]	[Insert position]	[Insert name of party]

- 3) Our specific responsibilities will be the following;
  - a) Making sure the [named] party abides by the sections of this Protocol.
  - b) Ensuring that all DO's and other staff are fully aware of their responsibilities.
  - c) Appointing other staff in the body to act as DO's in their absence.
  - d) Authorising the [named] body's involvement and co-operation in the information sharing process, at every stage.
  - e) Keeping a Protocol Co-ordination Folder, which holds all the partner's information sharing documents in general.
  - f) Ensuring the [named] body's Data Protection Notification entry is accurate, up to date and adequate for the purpose for which it is intended.
- 4) [The appointment of the PDO needs to be confirmed in writing and stored on the Protocol Co-ordination Folder, for all partners to see].
- 5) Only [names] DO's and PDO's of [name] body can make the formal requests and document agreements for the sharing of personal information. We can decide (on a case by case basis,) why a disclosure is necessary to support action under the Crime and Disorder Act 1998. We will also decide why and when the public interest overrides the presumption of confidentiality.

- 6) It is our responsibility to ensure that processing of the personal data held, is in keeping with the principles of the Data Protection Act 1998, namely;
  - a) It is obtained, processed and disclosed fairly and lawfully.
  - b) Kept securely.
  - c) Processed in accordance with the rights of the data subjects.
  - d) Accurate, relevant and held no longer than necessary.
  - e) Disclosed only for a specified related purpose.
  - f) Disclosed without the subject's knowledge and/or agreement only where failure to do so would prejudice the objective.
  
- 7) We will create a project folder or file [\[another term may be used here\]](#) to ensure ease of administration, covering all aspects and documentation of the information sharing process. This folder or file will be managed by us [\[name\]](#) PDO or DO's, to ensure that it is accurate and up to date. We must ensure that the information held is reviewed with our partners by arrangement [\[insert agreed period\]](#), but at least quarterly.
  
- 8) The folder or file must include;
  - a) Record of data disclosed
  - b) Project chronology
  - c) Project access list
  - d) Notes of meetings with our partners, and recent correspondence and phone calls.
  
- 9) We [\[name\]](#) PDO or DO are the data owners. As such, any final decision or whether to share sensitive information, rests with us.

## PROCESS SECTION

- 1) We will define the requirement, outline the nature of the risk, identify the information holders and agree future disclosure procedures. It is this initial contact between us whether by meeting, correspondence or telephone, that is fundamental to the drawing-up of this Protocol. **This process may involve meetings, but the process must be documented in writing. This is to provide a paper trail for any audit and for clarity purposes.**
- 2) Agreed disclosure procedures will generally require making a request in writing. The reply to this request will normally be made within [\[insert timeframe\]](#). As the disclosing partner, it is my responsibility to make the assessment and consider the nature of the formal request, replying within [\[Insert time-frame\]](#).
- 3) Access to personal information by staff other than ourselves [\[as PDO or DO\]](#), should be limited to employees whose work is directly related to the project and those working within the crime reduction program or field.
- 4) The data subject is legally entitled to request their records from the receiving agency unless an exemption under the Data Protection Act 1998 applies. If the subject requests access to their records, we should immediately contact the disclosing agency, to determine whether the latter wishes to claim exemption. From this stage, the procedure should be fully documented in writing and stored on file.
- 5) We must agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice [\[insert here\]](#). This should cover variations of data held by us and we should agree a maximum retention period for each item of data.

[\[It must be noted that the above represents the recommended approach to setting-up data sharing arrangements. You may have less formal arrangements.\]](#)

## SECURITY & DATA MANAGEMENT SECTION

- 1) It is our responsibility as signatories to this Protocol, to ensure that we have adequate security arrangements in place, in order to protect the integrity and confidentiality of the information we hold.
- 2) We agree that personal information disclosed must;
  - a) Not be emailed over internet links, where this is practical.
  - b) Be protected by back-up rules.
  - c) When stored on a computer system, it must be password protected and we agree this password will be revised regularly.
  - d) When manual, be stored in a secure filing cabinet when not in use.
  - e) Be located in a geographically secure environment.
  - f) Not be inputted/accessed without industry standard security devices as defined by BS7666.
- 3) **The national standard for making data “fit for use” is industry standard BS 7666.** This is the standard for describing the location of types such as addresses, rights of way and streets. As most public sector data has a location element to it, this is a good standard to convert disparate data sets from different systems and agencies and fully integrate them. [\[All data sharing initiatives complying with BS 7666 will dovetail into Modernising Government policy initiatives on a local level, such as Call Centres, Data Warehouses and One Stop Shops.\]](#) We agree that in order to “future proof” this Protocol, we undertake to use industry standard BS7666 to process our data.
- 4) All data held by us is subject to a specified “shelf-life.” [\[to be agreed here\]](#). All personal data disclosed to us will be held until [\[describe when data no longer required for purposes of partnership\]](#).
- 5) We understand that all these measures need to be taken to ensure the security of our partners and to protect the general public.
- 6) We are aware that only the minimum amount of information should be disclosed, in order to get the job done and for the purpose for which it was intended. We agree that all information retained by us and our partners should be kept securely and for not longer than is strictly necessary.

## COMPLAINTS AND BREACHES SECTION

### **Complaints:**

- 1) Initial complaints must be referred to the appropriate PDO or DO [insert names] and we agree in this Protocol, the procedure to be followed in the event of such a complaint being received, is as follows; [insert your agreed procedure].
- 2) We agree that any formal complaint by a data subject regarding any stage of the process will be notified (as a best practice measure) in writing to all of our partners.
- 3) We undertake to do all that we can within the guidelines of the Data Protection Act 1998, to assist with any complaint.
- 4) Individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman. [The local addresses may be inserted into the Appendix].

### **Breaches:**

- 5) We agree that any breach of confidentiality will seriously undermine and affect the credibility of crime audit work, our partnership objectives, and render us liable for breach of the law.
- 6) We undertake at all times, to comply with data protection and other legal requirements relating to confidentiality.

## **AUDIT SECTION**

- 1) **Audit of Data:** We undertake to ensure that we will collect, process, store and disclose all data held by us, within the terms of this Protocol and the relevant legislation. We agree to ensure that all information held by us, is accurate, relevant and fit for the purpose for which it is intended.
  
- 2) **Audit of Security:** We agree to store all held data securely as per the terms of the Security and Data Management section. We will dispose securely of all data held. We also pledge to conduct six-monthly audits of our security arrangements, to ensure they are effective.
  
- 3) **Audit of Protocol:** We undertake to conduct regular audits of this Protocol at [\[agree here\]](#) fixed periods, in order to amend it and ensure it remains fully effective.

**SIGNATORIES SECTION**

This Protocol [\[insert title here\]](#), must be signed by a representative of sufficient standing from each of the named parties, in the following format:

**AGREEMENT**

SIGNED \_\_\_\_\_  
[\[Type of Official-see below\]](#) For and on behalf of [\[named party\]](#) Date

SIGNED \_\_\_\_\_  
[\[Type of Official-see below\]](#) For and on behalf of [\[named party\]](#) Date

[\[Repeat the above process until a representative from each named party on this Protocol is included\]](#)

[\[Choose from this list of Designated Officers\]](#)

- 1) DIVISIONAL COMMANDER
- 2) CHIEF EXECUTIVE
- 3) CHIEF PROBATION OFFICER
- 4) HEALTH AUTHORITY CHIEF EXECUTIVE
- 5) PROPER DESIGNATED OFFICER
- 6) CHALCOTT GUARDIAN
- 7) STRATEGIC DIRECTOR
- 8) HOUSING MANAGER
- 9) COMMUNITY SAFETY OFFICER
- 10) COMMUNITY SAFETY INSPECTOR
- 11) OTHER TITLE [\[insert here\]](#)

## GLOSSARY TO THE PROTOCOL SECTION

[It must be noted that the Protocol should be written in as plain and clear English as possible].

[Insert as many terms as are relevant to your Protocol from this list].

- ACCESS LIST:** A register specific to a project where personal information is shared logging the authorised access to the information.
- AGENCIES:** Those signatories party to this Protocol which for the time being are prescribed by order of the Secretary of State under a duty to formulate and implement crime and disorder strategies in compliance with the Crime and Disorder Act 1998.
- AGGREGATE DATA:** Data that consists of statistics of events forming a trend or pattern but from which it is not possible to identify individuals.
- ANTI-SOCIAL BEHAVIOUR:** 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.
- AUDIT TRAIL:** A process of collating data for the purpose of identifying and refining internal procedures of partner agencies, by means of examination of all documentation kept on the information exchange.
- BULK TRANSFER:** The disclosure of a quantity/set of identifiable personal data, for the purpose of a criminal investigation/ crime and disorder initiative.
- COMMON LAW:** The principle underlying all criminal-related work is the common law duty of confidentiality owed to the public. This requires that personal information given for one purpose cannot be used for another, and places restrictions on the disclosure of that information. This duty can only be broken if the public interest requires it. Statutory provisions on disclosure override common law provisions.
- COMMUNITY SAFETY MANAGEMENT GROUP:** A multi-agency group that manages the practical development and implementation of the crime & disorder strategy.
- CONSENT:** Agreement, either expressed or implied, to an action based on knowledge of what that action involves, its likely consequences and the option of saying no.
- EXPRESS CONSENT:** Consent which is expressed orally, or in writing, (except where patients cannot write or speak, when other forms of communication may be sufficient.)
- CRIME:** Any act, default, or conduct prejudicial to the community, the commission of which by law, renders the person responsible liable to punishment by fine, imprisonment or other penalty.
- CRIME AND DISORDER ACT 1998:** The purpose of the Act is to tackle crime and disorder and help create safer communities. It requires the police and local authorities in partnership with the community, to establish a local partnership to cut crime. This partnership must

- conduct an audit to identify the types of crime in the area and develop a strategy for tackling them.
- CRIME AUDIT:** A process of collating statistical data from lawful sources to identify trends or patterns in crime and disorder in order to formulate strategies and projects to disrupt and negate criminal and anti-social behaviour.
- CRIME MAPPING:** This is the process of combining data resources and the use of different types of data, to create a more accurate or clear picture of what is going on in the area.
- DATA:** Essentially the same as “information,” but tends to be information recorded in a form, which can be processed by equipment automatically (usually electronically), in response to specific instructions.
- DATA IN THE PUBLIC DOMAIN:** Any information which is publicly available, whether it relates to a living individual or not. For example, Information found on the internet, television or local authority records.
- DATA OWNER:** This is the individual or partner who is responsible for complying with the eight Data Protection principles, as set-out in the Data Protection Act 1998. It is the owner’s responsibility to ensure that the data is securely stored.
- DATA PROCESSING:** This term is used to describe the collecting, handling, sanitising, transferring and storing of all types of data.
- DATA PROTECTION ACT 1998:** A major piece of legislation, governing who can store data and share it and under which circumstances. It embodies the eight basic principles of data processing, and gives guidance on data sharing.
- DATA SHARING (EXCHANGE):** The physical exchange of data between one or more individuals or agencies; this is data recorded in an electronic or processing form. For example, this usually involves the transfer of a data set to a partner agency.
- DATA SUBJECT:** An individual who is the subject of personal data, being data from which a living individual can be identified.
- DE-PERSONALISED DATA:** This is information where any reference to or means of identifying a living individual has been removed or “sanitised.”
- DESIGNATED OFFICER:** A person nominated by the agency of sufficient standing, to process or initiate requests for personal information and data. [Health Authority representatives may refer to them as “Caldicott Guardians”].
- PRIMARY DESIGNATED OFFICER:** As Designated Officer, only the most senior member of the information sharing party in the partnership.
- DISORDER:** Refers to the level or pattern of anti-social behaviour within a certain area.
- EDUCATION ACTION ZONE:** Geographical area identified as being beneficiary of government funding, providing local businesses contribute a set amount for precise education needs
- FORMAL REQUEST:** A written request by the Designated Officer for personal information made to the information holder.
- HEALTH ACTION ZONE:** Geographic area identified as being beneficiaries of government funding to address significant health inequalities.

- HOT SPOT AREAS:** These are geographic areas of focus, where there is a disproportionately above average incidence of criminal activity.
- HUMAN RIGHTS ACT 1998:** This Act requires the compliance to Article 8 of the European Convention on Human Rights. This allows interference with the right to respect for private and family life only when it is in accordance with the law, and pursues a legitimate public interest in a proportionate manner.
- INDEMNITY:** Parties may seek to indemnify themselves against eventual legal action or litigation for compensation for damage or distress under the relevant legislation.
- INDIVIDUAL:** A person not being covered by the definition of an agency, but who has assumed or has been invited by the agencies to assume a role in the project which is the object of this Protocol.
- INFORMATION:** This is essentially the passing of knowledge from one party to another in this Protocol.
- INFORMATION OBTAINED FOR NATIONAL STATISTICS:** Refers to administrative and survey data. Used within the NS framework.
- INFORMATION SHARING (EXCHANGE):** Involves a physical exchange of data between one or more individuals or agencies.
- INTELLIGENCE:** This is the end product of a process by which that information is checked and compared with other information and is then used to inform decision-making.
- LOCAL POLICING UNIT:** An area covered by one police station.
- MAINSTREAMING:** To provide services as part of the usual business of an organisation, rather than as a short-term project or initiative.
- MEMORANDUM OF UNDERSTANDING:** Essentially, another term for Protocol.
- META-DATA:** This is essentially data about data. This is a process of making the finding of a resource more efficient, by providing a structure of defined elements that describe or catalogue the resource. It should also provide details as to how the elements are used.
- NON-DOMESTIC BURGLARY:** All burglary that does not occur in a residential property. Includes burglary against sheds and garages, public buildings, commercial property.
- NON-PERSONAL INFORMATION:** Any information which does not or cannot be used to establish the identity of a living individual.
- PERFORMANCE INDICATOR:** Tool to measure the success/failure of an objective
- PERSONAL INFORMATION:** Information which relates to a living individual who can be identified from the data or any other information which is in the possession of the data holder. This is the most restricted type of information and should only be used where there is no reasonable alternative.
- PERSONAL INFORMATION REQUEST FORM (PIRF):** A form requiring the disclosure of personal information from the information holder.
- PROJECT:** A planned and co-operative activity undertaken by agencies and individuals to disrupt and negate criminal and antisocial behaviour according to the precepts of the Crime and Disorder Act 1998.
- PROJECT CHRONOLOGY:** A register specific to a project where each agency logs its involvement in the information sharing process and the security arrangements.

- PROJECT FILE:** A file to be kept by each partner agency containing all the personal information and documentation relevant to the information sharing process for the project.
- PROJECT GROUP:** Individuals and agency representatives formed into a group to manage a project.
- PROJECT MEETING:** Meeting of the project group, to discuss the project.
- PROTOCOL CO-ORDINATION FOLDER:** To be held by each partner agency giving an overview of its information sharing arrangements and all projects in which it is involved.
- PUBLIC DOMAIN:** Information is judged to be in the public domain when it is so generally accessible that it can no longer be regarded as confidential.
- RECORDED OBJECTIVES:** The objectives formulated, outlined and agreed in an initiation document by the agencies as the beginning of a project under this Protocol.
- RELEVANT AUTHORITIES:** Any of these bodies or persons referred to in Section 115 (2) of the Crime and Disorder Act 1998, and described in detail in section 5 (1), (2), and (3).
- REVIEW:** Periodic review of data exchanged for the purposes of the project including review of the scope, relevance and accuracy of disclosed data; a review process which shall be defined at the time of the project initiation.
- RISK ASSESSMENT:** Carried out to establish whether the subject is likely to commit serious, physical, psychological harm to others.
- RISK MANAGEMENT:** A plan to reduce, manage or eliminate the risk. The components may include **treatment, supervision, incapacitation, disclosure.**
- RISK SCREENING:** The initial process of confirming information. The degree of likelihood and gravity of consequences of future behaviour.
- SMART:** Specific, Measurable, Achievable, Realistic with a Timetable.
- SCOPING:** Liaison between partner agencies, before a formal request is made, to define the problem and identify information holders.
- TRIGGER EVENT:** Information received by an agency that indicates an individual may constitute a risk of harm. Or which viewed together with other information, leads to that view.
- TWOC:** Taking a car without the owner's consent.

## APPENDIX SECTION

[In this very large section, place all relevant or pertinent documents and forms.]

For example, choose from the following list;

- 1) The request for information forms, filled in by the enquiring party. [\[Insert here\]](#).
- 2) The Personal Information Request Forms (PIRF), filled in by the disclosing party. [\[Insert here\]](#)
- 3) The Human Rights Act 1998, definitions and articles. [\[Insert here\]](#).
- 4) The Data Protection Act 1998, definitions, sections and implications. [\[Insert here\]](#).
- 5) The Crime and Disorder Act 1998, definitions, implications and relevant sections (section 115 & section 17). [\[Insert here\]](#).
- 6) Guidance from the General Medical Council on Patient Confidentiality, definitions and relevant sections. [\[Insert here\]](#)
- 7) The Freedom of Information Act 2000, definitions, relevant sections and implications on data-sharing. [\[Insert here\]](#)
- 8) Any other relevant legislation, such as the Mental Health Act or the Housing Act 1996. [\[Insert here\]](#)
- 9) Any guidance on which bodies are entitled and invited to form the Crime Reduction Partnership. [\[Insert table 1 here\]](#). Types of Information.
- 10) Notes for specific Guidance, that are too bulky to be placed in the main text of this Protocol. For example, the day to day operation and procedures of the partnership, including the posts responsible for producing information, content and format of data, and means of exchanging data. [\[Insert here\]](#).
- 11) Library of good example Information Sharing Protocols