

**NEWHAM
CRIME & DISORDER
REDUCTION PARTNERSHIP**

**PROTOCOL AND PROCEDURE FOR THE
EXCHANGE OF INFORMATION
As Amended 9th June 2008**

AGREED BETWEEN:

**ARHAG Housing Association
ASRA Greater London Housing Association
British Transport Police
Circle 33 Housing Trust
Community HA (One Housing Group)
Dominion Housing Group
East Thames Group
English Churches Housing Group
Family Mosaic
Gateway Housing Association
Genesis Housing group
Habinteg Housing Association
Home from Home Housing Association
Kush Housing Association
London & Quadrant Housing Association
London Borough of Newham
London Fire Brigade
London Probation
Look Ahead Housing and Care
Metropolitan Police
NCH
Network Housing group
Newham Homes
Newham NHS Primary Care Trust
Newham University Hospitals Trust
North London Muslim Housing Association
Notting Hill Housing Trust
Peabody Trust
Pinnacle
Single Homeless Project
Southern Housing Group
Toynbee Housing Association (One Housing Group)
Westminster Drugs Project**

CONTENTS

CONTENTS 3
INTRODUCTION 4
“GOLDEN RULES” SECTION 6
Type of Data 7
NON-PERSONAL DATA 9
DE-PERSONALISED DATA 9
Statutory Disclosure of De-Personalised Data 10
PERSONAL DATA 10
COMMON LAW DUTY OF CONFIDENTIALITY 11
SENSITIVE DATA 14
INDEMNITY 15
PRIMARY DESIGNATED OFFICERS 16
SECURITY & DATA MANAGEMENT 18
COMPLAINTS AND BREACHES 19
AUDIT SECTION 20
Designated Officers 20
GLOSSARY TO THE PROTOCOL 21
APPENDIX A 25
APPENDIX B: SI 2007 NO. 1830 38
APPENDIX C, SI 2007 No, 1831 46
INTER AGENCY INFORMATION REQUEST AND RESPONSE FORM 51

INTRODUCTION

- 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:-
 1. Anti-Social Behaviour Orders
 2. Child Safety Orders
 3. Detention and Training Orders
 4. Drug Treatment and Testing
 5. Local Child Curfew Schemes
 6. Parenting Orders
 7. Seizure of noise-making equipment
 8. Car crime
 9. Racially aggravated offences
 10. Reparation Orders
 11. Removal of truants
 12. Supervision Orders
 13. Youth Courts
 14. Youth Justice Plans
 15. Youth Offending Teams
 16. Sex Offender Orders
 17. The reduction of crime and disorder in the area
 18. Reprimands and warnings (and cautions/supported cautions in the interim period)
- 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.
 - a) **Common Law Duty of Confidence [social services, medical profession patient confidentiality, police]**
 - b) **The Freedom of Information Act 2000**

- c) The Housing Acts**
 - d) The Mental Health Act 1983**
 - e) Health & Social Care Act 2001**
 - f) Education Act 1996**
 - g) Children Act 1989**
 - h) NHS and Community Care Act 1990**
 - i) Sex Offenders Act 1997**
 - j) Anti-Social Behaviour Legislation**
 - k) Any other relevant Legislation.**
- 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 signatories to this Protocol of 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 May 2007 and annually thereafter, and any comments should be sent to the appointed Primary Disclosure Officer (PDO) for each party to this protocol
- 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.

“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 to 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, The Freedom of Information Act 2000 and in accordance with the Home Office guidance associated with these Acts.
- 3) We pledge to consult with each-other annually upon matters of policy and strategy for the sharing of information.
- 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 10 days where it is non-urgent and within 48 hours (2 working days) for urgent requests; 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. The partner receiving the data will not use it for any purpose other than that as set-out in this Protocol, nor share it with any other party, without the disclosing partner’s written permission. *There shall be no secondary disclosure without the written permission of the disclosing partner unless specific legislation allows such secondary disclosure.*
- 6) Each Party to this Protocol undertakes to ensure that it complies with all relevant legislation, this Protocol, and its internal policies on **disclosure**. Parties must seek their own legal advice, wherever necessary.
- 7) We agree to disclose information to primary designated officers and designated officers only of relevant authorities or who are acting on behalf of a relevant authority for the purposes of the Crime and Disorder Act 1998 and have signed this Protocol. 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 is not allowed

and a new consent should be obtained , from that body in the proper manner.

- The permission of the Police must always be obtained for data provided by the Police before any secondary disclosure is made.

8) The information disclosures can consist of(this list is not exhaustive):

Source	<u>TYPE OF DATA</u>
Police	Crime incidents, recorded crime statistics, ACPO defined disorder incidents Offender information, witness details where consent has been obtained, conviction data Victim information, evidence to support court proceedings e.g. statements, officer attendance Command & control data on non-crime incidents
Police Authority	Public surveys
Local Authority	Housing voids, damage to non housing property and land, anti-social behaviours orders, RSLs Criminal damage costs, derelict property, emergency property, entry phones, evictions Neighbourhood complaints, property rooms, re-housed offenders, re-housed homeless Vandalism records, types of locks and fittings, sub-standard housing, re-housed victims Racial/homophobic incidents, emergency out of hours calls, empty property, turnover of tenants Reasons for transfer applications Records of neighbour disputes/complaints Stock turnover, rent arrears and possessions, housing and council tax benefits Evictions, injunctions, relating to anti-social behaviour Previous addresses Persons in occupation within premises Information on vulnerable groups e.g. elderly, people with disabilities mentally ill, child protection, child abuse, lone parents, families on benefit Children in care/leaving care, child neglect, low family income and deprivation Information on young offenders, nuisance families, needle exchange, welfare referrals Exclusions Truancy Others on school premises including those without permission Grant applications School registrations data/ records Addresses of families Experience of discipline

	<p>Neighbourhood disputes Refuse collections problems, fly tipping, dogs fouling, strays, dangerous, barking Health & Safety problems, notices and prosecutions, odour, pollution, drainage, food Grants for safety improvements, pollution, licensing, gambling premises, public houses Statutory nuisances Noise nuisance complaints Records of unlicensed and abandoned vehicles Information about registered keepers of vehicles All night cafes, diseases, households, educational establishments, complaints origin, commercial property types Location of traffic accidents Requests for lighting Census data analysis Needs analysis for external grants Records of crime/anti-social behaviour against staff Planning maps Previous area based work Forthcoming developments Census data</p>
Probation	<p>Land use, including dereliction, recreational, and business Offender profiles e.g. age, gender, employment status, substance misuse, reconviction data, percentage of risk cases, effectiveness of programs, types of orders, total case loads, offender needs e.g. drugs. Housing supervision status, release from custody/licence information, risk assessment</p>
Strategic Health Authority / Primary Care Trusts	<p>Health Morbidity data</p>
Drug Action Team	<p>Information on drug-taking/alcohol & substance misuse</p>
Fire Service	<p>Incidents of arson, hoax calls, suspicious fires</p>
All public buildings e.g. schools, hospitals, libraries and leisure facilities	<p>Costs of criminal damage and vandalism</p>
RSLs	<p>Similar information as for Local Authorities</p>

9) Each party to this protocol 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

- 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.

DE-PERSONALISED DATA

- 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 anonymous data about them may be used (particularly for sample healthcare patients.)

STATUTORY DISCLOSURE OF DE-PERSONALISED DATA

The Responsible Authorities, as defined in section 5 of the Crime and Disorder Act 1998 ("1998 Act") as amended, shall comply with their statutory duty to disclose depersonalised information pursuant to the Crime and Disorder (Prescribed Information) Regulations 2007 as annexed hereto. The disclosure shall be to all Relevant Authorities as required by section 17A of the 1998 Act.

PERSONAL DATA

- 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.

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.
- b) The conditions of schedule 2 of the Data Protection Act 1998 must be satisfied.
- c) The proposed disclosure of personal information can be done in accordance with the principles of the Data Protection Act 1998.

- d) We can disclose personal information reflecting the (i) common law duty of confidentiality and (ii) the principles of the Human Rights Act 1998:-

COMMON LAW DUTY OF CONFIDENTIALITY

Where an individual has given their clear and explicit consent to disclosure for a particular purpose, the common law duty of confidence is overcome. Crime Reduction is one area, where seeking the individual's consent is not always appropriate, for example, the detection of crime. Information held in confidence can still be disclosed without the individual's consent, where it can be demonstrated that:

- disclosure is required by law (e.g. under an Act of Parliament creating a statutory duty to disclose).
- for the detection, prevention and prosecution of serious crime.
- there is a public interest.
- there is a risk of death or serious harm
- a public health interest.
- in the interest of the individual's health.
- In the interest of the individual concerned.

It will need to be clearly established that these considerations are sufficient to override the duty of confidence and that the disclosure is strictly necessary for these purposes.

In the context of mainstream crime reduction activities, the majority of disclosures are normally considered to be in the public interest. This should be particularly true of the activities outlined in the Crime & Disorder Act 1998 (see Crime & Disorder Activities). The very wide range of crime reduction activities and the need to consider individual circumstances means that it is not possible to provide clear or authoritative advice in this guidance and legal advice must be sought, where there is any doubt. Case Law on the disclosure of information in this context should also be given full consideration and will highlight relevant considerations.

The police have a general common law power to disclose information for policing purposes, usually for one or more of the following reasons,

- prevention and detection crime
- apprehension and prosecution of offenders
- protection of life and property
- licensing and vetting
- assisting the public

Disclosures for any of these reasons are normally detailed in guidance within force policies and procedures. Section 115 of the Crime & Disorder Act provides this power, where it is necessary for a purpose defined by and compliant with the Act (see Crime & Disorder Activities).

Having established that there are legal grounds for disclosure in common law, compliance with relevant statute law (i.e. Data Protection Act 1998, Crime &

Disorder Act 1998, Human Rights Act 1998 and other relevant legislation) will need to be established.

Human Rights Act 1998: see appendix.

- 3) 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.
- 4) 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.

-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.
- 5) **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.
- 6) 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.

7) **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.

8) **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 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.

9) **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.

10) **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.

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. Details of cautions and convictions may be disclosed for use in possession proceedings to establish anti-social behaviour.

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 and other relevant anti-social behaviour legislation. 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.

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 and other anti-social behaviour legislation.

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 and other relevant anti-social behaviour legislation.
- 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

- 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:** (for disclosure of sensitive data)

Where appropriate and possible, express written 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.***

INDEMNITY

In consideration of the provision of information in accordance with this protocol, partner agencies undertake to indemnify any person or a partner agency against any liability which may be incurred by such a person or partner agency arising from, or in any way connected with, the following acts

or omissions on the part of the person or partner agency granting the indemnity:

- a) requests for information for purposes other than those specified in the joint protocol
- b) use of the information for purposes other than those specified in the joint protocol
- c) disclosure of the information to a third party except insofar as it is strictly necessary for the purposes of any legal proceedings pursuant to the Crime & Disorder Act 1998.

Any disclosure of information by an employee, which is done in bad faith, or for motives of personal gain will be the subject of an inquiry conducted by the employer of such an employee, and will be treated as a serious disciplinary matter. Each party partner agency shall be accountable for any misuse of the information supplied to that party and the consequences of such misuse by its employees, servants or agents.

PRIMARY DESIGNATED OFFICERS

- 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 Schedule 1.
 - 2) The named individuals within Schedule 1 are designated to assume responsibility for data protection (including notification where appropriate), security and confidentiality, and compliance with all relevant legislation; and it is agreed that any change of Primary Designated Officer shall be notified in writing to every other party to this protocol within 5 working days of such change occurring.
- 2) Our specific responsibilities will be the following;
- a) Making sure the signatories to this Protocol abide 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 an individual 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 that each signatory'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 must be confirmed in writing, which includes notification by electronic email, to the London Borough of Newham, and stored on the Protocol Co-ordination Folder
- 3) Only Designated Officers and PDO's of each Party to this Protocol 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.
- 4) 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.
- 5) We will create a project folder or file [another term may be agreed by the parties in writing] to ensure ease of administration, covering all aspects and documentation of the information sharing process. This folder or file will be managed by us the named 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 quarterly.
- 6) 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.
- 7) We the PDO's are the data owners. As such, any final decision on whether to share sensitive information, rests with us.

INFORMATION PROCESS

- 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 10 working days for non-urgent requests and within 48 hours (2 working days) for urgent requests. As the disclosing partner, it is my responsibility to make

the assessment and consider the nature of the formal request, replying within the time limits set out above.

- 2A) Information may be requested or provided by using a secure electronic email network. The decision on whether to use email will be made by the data owner.
- 3) Access to personal information by staff other than the Primary Designated Officers and Designated Officers will 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 agree the criteria for the review and weeding of data in accordance with existing policies and codes of practice in accordance with this protocol and guidance from the Information Commissioner. This also covers variations of data held by us.

SECURITY & DATA MANAGEMENT

- 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 unsecured 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 secure environment in the U.K
 - 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 “shelf-life” after which it must be destroyed. All personal data disclosed to us will be held for a maximum of 12 months from date of receipt or a further extension of 12 months by agreement but shall be destroyed promptly at an earlier date soon as the purpose for which it has been obtained has been achieved except when retention of the data is necessary for a longer period of time to comply with requirements of legal proceedings or other statutory provisions. We will review the need to retain the disclosed data quarterly if not already destroyed.

4A) Each PDO agrees to provide an annual return of information requests received and information provided and the data will be sent to all PDOs for the time being named within Schedule 1 to the Protocol.

- 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

Complaints:

Initial complaints must be referred to the appropriate Primary Designated Officer for each body/ organisation and we agree in this Protocol, the procedure to be followed in the event of such a complaint being received, is that each partner shall apply its own adopted procedure for dealing with complaints

- 1) 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.
- 2) We undertake to do all that we can within the guidelines of the Data Protection Act 1998, to assist with any complaint.
- 3) Individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman.

Breaches:

- 4) 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.

- 5) We undertake at all times, to comply with data protection and other legal requirements relating to confidentiality.
- 6) where a breach occurs the Partner concerned shall review its procedures to prevent re-occurrence of the breach.

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 annually, in order to amend it and ensure it remains fully effective.

DESIGNATED OFFICERS

The parties agree to notify in writing any change of designated officers to every other party to this protocol within 5 working days of such change occurring.

Details of the designated officers for each Party are set out in Schedule 2.

GLOSSARY TO THE PROTOCOL

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	This Act requires the compliance to Article 8 of the European

ACT 1998:	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 A

19. The Request for Information Forms, filled in by the enquiring party.
We understand that non-personal data constitutes data that does not or cannot be used to establish the identity of a living individual. 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.
20. 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.
21. 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.

The Human Rights Act 1998,
definitions and articles.

- section 1. - (1) In this Act "the Convention rights" means the rights and fundamental freedoms set out in-
- (a) Articles 2 to 12 and 14 of the Convention,
 - (b) Articles 1 to 3 of the First Protocol, and
 - (c) Articles 1 and 2 of the Sixth Protocol,
- 1) as read with Articles 16 to 18 of the Convention.
 - (2) Those Articles are to have effect for the purposes of this Act subject to any designated derogation or reservation (as to which see sections 14 and 15).
 - (3) The Articles are set out in Schedule 1.
 - (4) The Secretary of State may by order make such amendments to this Act as he considers appropriate to reflect the effect, in relation to the United Kingdom, of a protocol.
 - (5) In subsection (4) "protocol" means a protocol to the Convention

ARTICLE 6 RIGHT TO A FAIR TRIAL

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or

the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
3. Everyone charged with a criminal offence has the following minimum rights:
 - (a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
 - (b) to have adequate time and facilities for the preparation of his defence;
 - (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
 - (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
 - (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

ARTICLE 7 NO PUNISHMENT WITHOUT LAW

1. No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed.
2. This Article shall not prejudice the trial and punishment of any person for any act or omission which, at the time when it was committed, was criminal according to the general principles of law recognised by civilised nations.

ARTICLE 8 RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Data Protection Act 1998

definitions, sections and implications:-

1. - (1) In this Act, unless the context otherwise requires-

"data" means information which-

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- (b) is recorded with the intention that it should be processed by means of such equipment,
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

"data controller" means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

"data subject" means an individual who is the subject of personal data;

"personal data" means data which relate to a living individual who can be identified-

- (a) from those data, or
- (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual;

"processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

"relevant filing system" means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

(2) In this Act, unless the context otherwise requires-

- (a) "obtaining" or "recording", in relation to personal data, includes obtaining or recording the information to be contained in the data, and
- (b) "using" or "disclosing", in relation to personal data, includes using or disclosing the information contained in the data.

(3) In determining for the purposes of this Act whether any information is recorded with the intention-

- (a) that it should be processed by means of equipment operating automatically in response to instructions given for that purpose, or
- (b) that it should form part of a relevant filing system,

it is immaterial that it is intended to be so processed or to form part of such a system only after being transferred to a country or territory outside the European Economic Area.

(4) Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.

Sensitive personal data.

2. In this Act "sensitive personal data" means personal data consisting of information as to-

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The special purposes.

3. In this Act "the special purposes" means any one or more of the following-

- (a) the purposes of journalism,
- (b) artistic purposes, and
- (c) literary purposes.

The data protection principles.

4. - (1) References in this Act to the data protection principles are to the principles set out in Part I of Schedule 1.

(2) Those principles are to be interpreted in accordance with Part II of Schedule 1.

(3) Schedule 2 (which applies to all personal data) and Schedule 3 (which applies only to sensitive personal data) set out conditions applying for the purposes of the first principle; and Schedule 4 sets out cases in which the eighth principle does not apply.

(4) Subject to section 27(1), it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.

Application of Act.

5. - (1) Except as otherwise provided by or under section 54, this Act applies to a data controller in respect of any data only if-
- (a) the data controller is established in the United Kingdom and the data are processed in the context of that establishment, or
 - (b) the data controller is established neither in the United Kingdom nor in any other EEA State but uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom.
- (2) A data controller falling within subsection (1)(b) must nominate for the purposes of this Act a representative established in the United Kingdom.
- (3) For the purposes of subsections (1) and (2), each of the following is to be treated as established in the United Kingdom-
- (a) an individual who is ordinarily resident in the United Kingdom,
 - (b) a body incorporated under the law of, or of any part of, the United Kingdom,
 - (c) a partnership or other unincorporated association formed under the law of any part of the United Kingdom, and
 - (d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the United Kingdom-
 - (i) an office, branch or agency through which he carries on any activity, or
 - (ii) a regular practice;
- and the reference to establishment in any other EEA State has a corresponding meaning.

SCHEDULE 1
THE DATA PROTECTION PRINCIPLES PART I
THE PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless-
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PART II INTERPRETATION OF THE PRINCIPLES IN PART I

The first principle

1. - (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
(2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who-
 - (a) is authorised by or under any enactment to supply it, or
 - (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.
2. - (1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless-
 - (a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and
 - (b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).
(2) In sub-paragraph (1)(b) "the relevant time" means-
 - (a) the time when the data controller first processes the data, or
 - (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged-
 - (i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,
 - (ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or
 - (iii) in any other case, the end of that period.

- (3) The information referred to in sub-paragraph (1) is as follows, namely-
- (a) the identity of the data controller,
 - (b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
 - (c) the purpose or purposes for which the data are intended to be processed, and
 - (d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3. - (1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.

- (2) The primary conditions referred to in sub-paragraph (1) are-
- (a) that the provision of that information would involve a disproportionate effort, or
 - (b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. - (1) Personal data which contain a general identifier falling within a description prescribed by the Secretary of State by order are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description.

- (2) In sub-paragraph (1) "a general identifier" means any identifier (such as, for example, a number or code used for identification purposes) which-
- (a) relates to an individual, and
 - (b) forms part of a set of similar identifiers which is of general application.

The second principle

5. The purpose or purposes for which personal data are obtained may in particular be specified-
- (a) in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or
 - (b) in a notification given to the Commissioner under Part III of this Act.

6. In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

The fourth principle

7. The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where-

- (a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, and
- (b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.

The sixth principle

8. A person is to be regarded as contravening the sixth principle if, but only if-
- (a) he contravenes section 7 by failing to supply information in accordance with that section,
 - (b) he contravenes section 10 by failing to comply with a notice given under subsection (1) of that section to the extent that the notice is justified or by failing to give a notice under subsection (3) of that section,
 - (c) he contravenes section 11 by failing to comply with a notice given under subsection (1) of that section, or
 - (d) he contravenes section 12 by failing to comply with a notice given under subsection (1) or (2)(b) of that section or by failing to give a notification under subsection (2)(a) of that section or a notice under subsection (3) of that section.

The seventh principle

9. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to-
- (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
 - (b) the nature of the data to be protected.
10. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.
11. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-
- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and
 - (b) take reasonable steps to ensure compliance with those measures.
12. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-
- (a) the processing is carried out under a contract-
 - (i) which is made or evidenced in writing, and
 - (ii) under which the data processor is to act only on instructions from the data controller, and
 - (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

The eighth principle

13. An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to-

- (a) the nature of the personal data,
- (b) the country or territory of origin of the information contained in the data,
- (c) the country or territory of final destination of that information,
- (d) the purposes for which and period during which the data are intended to be processed,
- (e) the law in force in the country or territory in question,
- (f) the international obligations of that country or territory,
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
- (h) any security measures taken in respect of the data in that country or territory.

14. The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Secretary of State may by order provide.

15. - (1) Where-

- (a) in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the European Economic Area, and
- (b) a Community finding has been made in relation to transfers of the kind in question,

that question is to be determined in accordance with that finding.

(2) In sub-paragraph (1) "Community finding" means a finding of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive.

SCHEDULE 2

CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE:

PROCESSING OF ANY PERSONAL DATA

1. The data subject has given his consent to the processing.
2. The processing is necessary-
 - (a) for the performance of a contract to which the data subject is a party, or
 - (b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the data subject.
5. The processing is necessary-

- (a) for the administration of justice,
- (b) for the exercise of any functions conferred on any person by or under any enactment,
- (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
- (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. - (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

10) the common law of confidentiality and the principles of the Human Rights Act 1998:-

Where an individual has given their clear and explicit consent to disclosure for a particular purpose, the common law duty of confidence is overcome. Crime Reduction is one area, where seeking the individual's consent is not always appropriate, for example, the detection of crime.

Information held in confidence can still be disclosed without the individual's consent, where it can be demonstrated that:

- disclosure is required by law (e.g. under an Act of Parliament creating a statutory duty to disclose).
- for the detection, prevention and prosecution of serious crime.
- there is a public interest.
- there is a risk of death or serious harm
- a public health interest.
- in the individual's health.
- In the interest of the individual concerned.

It will need to be clearly established that these considerations are sufficient to override the duty of confidence and that the disclosure is strictly necessary for these purposes.

In the context of mainstream crime reduction activities, the majority of disclosures are normally considered to be in the public interest. This should be particularly true of the activities outlined in the Crime & Disorder Act 1998 (see Crime & Disorder Activities). The very wide range of crime reduction activities and the need to consider individual circumstances means that it is not possible to provide clear or authoritative advice in this guidance and legal advice must be sought, where there is any doubt. Case Law on the disclosure of information in this context should also be given full consideration and will highlight relevant considerations.

The police have a general common law power to disclose information for policing purposes, usually for one or more of the following reasons, the:

- prevention and detection crime
- apprehension and prosecution of offenders

- protection of life and property
- licensing and vetting
- assisting the public

Disclosures for any of these reasons are normally detailed in guidance within force policies and procedures.

Section 115 of the Crime & Disorder Act provides this power, where it is necessary for a purpose defined by and compliant with the Act (see Crime & Disorder Activities).

Having established that there are legal grounds for disclosure in common law, compliance with relevant statute law (i.e. Data Protection Act 1998, Crime & Disorder Act 1998, Human Rights Act 1998 and other relevant legislation) will need to be established.

(2) The Crime and Disorder Act 1998:

section 115 (1): Any person who, apart from this subsection, would not have the power to disclose information-

(a) to a relevant authority; or

(b) to a person acting on behalf of such an authority,

shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of any provision of this Act.

- 2) Guidance from the General Medical Council on Patient Confidentiality, definitions and relevant sections.

The Freedom of Information Act 2000,

definitions, relevant sections and implications on data-sharing.

PART I ACCESS TO INFORMATION HELD BY PUBLIC AUTHORITIES

Right to information General right of access to information held by public authorities.

1. - (1) Any person making a request for information to a public authority is entitled-

(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and

(b) if that is the case, to have that information communicated to him.

(2) Subsection (1) has effect subject to the following provisions of this section and to the provisions of sections 2, 9, 12 and 14.

(3) Where a public authority-

(a) reasonably requires further information in order to identify and locate the information requested, and

(b) has informed the applicant of that requirement,

the authority is not obliged to comply with subsection (1) unless it is supplied with that further information.

(4) The information-

(a) in respect of which the applicant is to be informed under subsection (1)(a), or

(b) which is to be communicated under subsection (1)(b),

is the information in question held at the time when the request is received, except that account may be taken of any amendment or deletion made between that time and the time when the information is to be communicated under subsection (1)(b), being an amendment or deletion that would have been made regardless of the receipt of the request.

(5) A public authority is to be taken to have complied with subsection (1)(a) in relation to any information if it has communicated the information to the applicant in accordance with subsection (1)(b).

(6) In this Act, the duty of a public authority to comply with subsection (1)(a) is referred to as "the duty to confirm or deny".

Effect of the exemptions in Part II.

2. - (1) Where any provision of Part II states that the duty to confirm or deny does not arise in relation to any information, the effect of the provision is that where either-

(a) the provision confers absolute exemption, or

(b) in all the circumstances of the case, the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing whether the public authority holds the information,

section 1(1)(a) does not apply.

(2) In respect of any information which is exempt information by virtue of any provision of Part II, section 1(1)(b) does not apply if or to the extent that-

(a) the information is exempt information by virtue of a provision conferring absolute exemption, or

(b) in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

(3) For the purposes of this section, the following provisions of Part II (and no others) are to be regarded as conferring absolute exemption-

(a) section 21,

(b) section 23,

(c) section 32,

(d) section 34,

(e) section 36 so far as relating to information held by the House of Commons or the House of Lords,

(f) in section 40-

(i) subsection (1), and

(ii) subsection (2) so far as relating to cases where the first condition referred to in that subsection is satisfied by virtue of subsection (3)(a)(i) or (b) of that section,

- (g) section 41, and
- (h) section 44.

Public Authorities.

- 3.** - (1) In this Act "public authority" means-
- (a) subject to section 4(4), any body which, any other person who, or the holder of any office which-
 - (i) is listed in Schedule 1, or
 - (ii) is designated by order under section 5, or
 - (b) a publicly-owned company as defined by section 6.
- (2) For the purposes of this Act, information is held by a public authority if-
- (a) it is held by the authority, otherwise than on behalf of another person, or
 - (b) it is held by another person on behalf of the authority.
- 3) Any other relevant legislation, such as the Mental Health Act or the Housing Act 1996.
- 4) Any guidance on which bodies are entitled and invited to form the Crime Reduction Partnership. Types of Information.
- 5) 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.
- 6) Library of good example Information Sharing Protocols

APPENDIX B: SI 2007 NO. 1830

Statutory Instrument 2007 No. 1830

The Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007

 STATUTORY INSTRUMENTS

2007 No. 1830**CRIMINAL LAW, ENGLAND**

The Crime and Disorder (Formulation and Implementation of Strategy)
Regulations 2007

<i>Made</i>	<i>22nd June 2007</i>
<i>Laid before Parliament</i>	<i>29th June 2007</i>
<i>Coming into force</i>	<i>1st August 2007</i>

The Secretary of State makes the following Regulations in exercise of the powers conferred by sections 6(2), (3), (4), (5) and 114 of the Crime and Disorder Act 1998^[1]:

Citation, commencement and extent

1. —(1) These Regulations may be cited as the Crime and Disorder (Formulation and Implementation of Strategy) Regulations 2007 and shall come into force on 1st August 2007.

(2) These Regulations extend to England only.

Interpretation

2. In these Regulations—

"area" means a local government area in England;

"community safety agreement" means an agreement prepared in accordance with regulation 9;

"co-operating persons and bodies" means persons or bodies co-operating in the exercise of responsible authorities' functions under section 5(2)^[2] of the 1998 Act;

"county area" means any county in England within which one or more of the councils for the districts are not unitary authorities;

"county strategy group" means a group established in accordance with regulation 8;

"crime and disorder" means crime and disorder including anti-social behaviour and other behaviour adversely affecting the environment;

"crime and disorder committee" means a committee established in accordance with section 19 of the Police and Justice Act 2006^[3];

"participating persons and bodies" means persons and bodies invited to participate in the exercise of the responsible authorities' functions under section 5(3)[4] of the 1998 Act;

"partnership monies" means monies provided by the Secretary of State and the responsible authorities for expenditure in accordance with the directions of the strategy group in support of the formulation and implementation of the strategic assessment and the partnership plan;

"partnership plan" means a partnership plan prepared under regulations 10 and 11;

"responsible authorities" means the responsible authorities for an area;

"strategic assessment" means an assessment prepared in accordance with regulations 5, 6 and 7;

"strategy group" means a group established in accordance with regulation 3;

"substance misuse" means the misuse of drugs, alcohol and other substances;

"the 1998 Act" means the Crime and Disorder Act 1998; and

"year" means a period of twelve months beginning on 1st April.

Functions in respect of the formulation and implementation of a strategy

3.—(1) For each area there shall be a strategy group whose functions shall be to—

(a) prepare strategic assessments; and

(b) prepare and implement a partnership plan;

for that area on behalf of the responsible authorities.

(2) Subject to paragraph (3) the members of the strategy group shall consist of one or more persons appointed from each responsible authority one of whom shall hold a senior position in that authority.

(3) Where the responsible authority referred to in section 5(1)(a) of the 1998 Act is a district council or a unitary authority and has an elected member responsible for community safety that member shall be one of the persons appointed under paragraph (2).

(4) The strategy group shall have in place arrangements governing the appointment of a chair, the period for which a person shall serve as chair and the grounds on which the chair may be removed during that period.

(5) The strategy group shall meet from time to time throughout the year as it considers appropriate.

(6) Strategy group meetings may be attended by persons who represent co-operating and participating persons and bodies and such other persons as the strategy group invites.

(7) At some point within each year the strategy group shall consider whether it, and those persons in the responsible authorities who work with

the strategy group, have the requisite knowledge and skills to exercise their functions under these Regulations.

(8) The strategy group shall have in place arrangements governing the review of the expenditure of partnership monies and for assessing the economy, efficiency and effectiveness of such expenditure.

Information Sharing

4. —(1) The strategy group shall have in place arrangements for the sharing of information between responsible authorities and shall prepare a protocol setting out those arrangements.

(2) The information sharing protocol shall relate to the sharing of information—

(a) under section 17A of the 1998 Act^[5];

(b) under section 115 of the 1998 Act^[6]; and

(c) otherwise for the purpose of formulating and implementing a strategic assessment and partnership plan for the area.

(3) Each responsible authority shall comply with the protocol prepared under paragraph (1) and each shall nominate a person within that authority to facilitate the sharing of information under the protocol.

Strategic Assessments

5. —(1) During each year the strategy group shall prepare a strategic assessment on behalf of the responsible authorities.

(2) The purpose of the strategic assessment is to assist the strategy group in revising the partnership plan.

6. In preparing the strategic assessment the strategy group shall consider—

(a) information provided to it by the responsible authorities;

(b) information provided to it by co-operating persons and bodies;

(c) information provided to it by participating persons and bodies;

(d) information provided to it by the crime and disorder committee for the area;

(e) the partnership plan for that year; and

(f) any other information relating to crime and disorder and substance misuse in the area given to the responsible authorities by persons living and working in the area.

7. A strategic assessment shall include—

- (a) an analysis of the levels and patterns of crime and disorder and substance misuse in the area;
- (b) an analysis of the changes in those levels and patterns since the previous strategic assessment;
- (c) an analysis of why those changes have occurred;
- (d) the matters which the responsible authorities should prioritise when each are exercising their functions to reduce crime and disorder and to combat substance misuse in the area;
- (e) the matters which the persons living and working in the area consider the responsible authorities should prioritise when each are exercising their functions to reduce crime and disorder and to combat substance misuse in the area;
- (f) an assessment of the extent to which the partnership plan for the previous year has been implemented; and
- (g) details of those matters that the strategy group considers should be brought to the attention of the county strategy group to assist it in exercising its functions under these Regulations.

Functions in respect of the formulation and implementation of a strategy at a county level

8. —(1) For each county area there shall be a county strategy group whose function shall be to prepare a community safety agreement for the county area on behalf of the responsible authorities in that county area.

(2) The members of the county strategy group shall consist of—

- (a) the chairs of each of the strategy groups for the areas within that county area;
- (b) where the council for that county area has an elected member responsible for community safety that member;
- (c) one or more persons appointed by the chief officer of police any part of whose police area lies within the county;
- (d) one or more persons appointed by the police authority any part of whose area so lies;
- (e) one or more persons appointed by the fire authority any part of whose area so lies; and

(f) one or more persons appointed jointly by the Primary Care Trusts the whole or any part of whose area so lies.

(3) The county strategy group shall have in place arrangements governing the appointment of a chair, the period for which a person shall serve as chair and the grounds on which the chair may be removed during that period.

(4) The county strategy group shall meet from time to time throughout the year as it considers appropriate.

(5) County strategy group meetings may be attended by persons who represent co-operating and participating persons and bodies for the areas in the county area and such other persons as the county strategy group invites.

Community Safety Agreements

9. —(1) Before the end of each year the county strategy group shall prepare a community safety agreement for that year.

(2) The community safety agreement shall be based on the strategic assessments for that year prepared by the strategy groups for the areas in the county area.

(3) The community safety agreement shall identify—

(a) the ways in which the responsible authorities in the county area might more effectively implement the priorities set out in these strategic assessments through coordinated or joint working; and

(b) how the responsible authorities in the county area might otherwise reduce crime and disorder or combat substance misuse through coordinated or joint working.

Partnership plans

10. —(1) The strategy group shall prepare a partnership plan for the area.

(2) Before the start of each year the strategy group shall revise the partnership plan.

(3) When revising the partnership plan the strategy group shall consider the strategic assessment and community safety agreement produced during the year prior to the year referred to in paragraph (2).

11. —(1) The partnership plan shall set out—

(a) a strategy for the reduction of crime and disorder and for combating substance misuse in the area in the three year period beginning with the year referred to in regulation 10(2);

(b) the priorities identified in the strategic assessment prepared during the year prior to the year referred to in regulation 10(2);

(c) the steps the strategy group considers it necessary for the responsible authorities to take to implement that strategy and meet those priorities;

(d) how the strategy group considers the responsible authorities should

allocate and deploy their resources to implement that strategy and meet those priorities;

(e) the steps each responsible authority shall take to measure its success in implementing the strategy and meeting those priorities; and

(f) the steps the strategy group proposes to take during the year to comply with its obligations under regulations 12, 13 and 14.

Community Engagement

12. —(1) For the purposes of preparing the strategic assessment and preparing and implementing the partnership plan the strategy group shall make arrangements for obtaining the views of persons and bodies who live or work in the area about—

(a) the levels and patterns of crime and disorder and substance misuse in the area; and

(b) the matters which the responsible authorities should prioritise when each are exercising their functions to reduce crime and disorder and to combat substance misuse in the area.

(2) The arrangements under paragraph (1) shall, so far as is reasonable, provide for consultation with—

(a) persons who appear to the strategy group to represent the interests of as many different groups or persons within the area as is reasonable; and

(b) persons who appear to the strategy group to represent the interests of those groups or persons within the area likely to be particularly affected by the implementation of the partnership plan.

(3) In making the arrangements under paragraph (1) the strategy group shall have regard to any other consultation with persons who live or work in that area that is undertaken by the responsible authorities in relation to the matters specified in sub-paragraphs 1(a) and (b) other than under these Regulations.

(4) The arrangements made under paragraph (1) shall provide that—

(a) the strategy group hold one or more public meetings during each year;

(b) that such meetings are attended by persons who hold a senior position within each of the responsible authorities;

(c) the strategy group shall take steps as it considers appropriate to bring to the attention of persons who live or work in the area, or who might otherwise be interested, information about(i) when such meetings are held; and

(ii) what was discussed at such meetings.

13. In preparing the partnership plan the strategy group shall consider the extent to which persons who live or work in the area might assist the

responsible authorities in reducing crime and disorder and substance misuse in the area.

14. The strategy group shall publish in the area a summary of the partnership plan in such form as it considers appropriate, having regard to the need to bring it to the attention of as many different groups or persons within the area as is reasonable.

Guidance

15. In exercising their functions under these Regulations the responsible authorities shall have regard to any guidance given by the Secretary of State.

Transitional provisions

16. —(1) Until the commencement of section 19 (local authority scrutiny of crime and disorder matters) of the Police and Justice Act 2006 regulation 6 shall have effect as if paragraph (d) were omitted.

(2) For the year beginning 1st April 2008 for the references in these Regulations to revising the partnership plan there shall be substituted preparing the partnership plan.

Scotland of Asthal, Q.C.
Minister of State
Home Office
22nd June 2007

EXPLANATORY NOTE

(This note is not part of the Regulations)

Section 5 of the Crime and Disorder Act 1998 ("the 1998 Act") gives certain public authorities in local government areas functions relating to the reduction of crime and disorder and the combating of substance misuse. Collectively these authorities are known as Crime and Disorder Reduction Partnerships (CDRPs). Section 6 of the 1998 Act places obligations on CDRPs to formulate and implement a strategy to reduce crime and disorder and combat substance misuse. These Regulations make further provision as to the formulation and implementation of that strategy.

Regulation 3 provides that CDRPs shall have a strategy group. The role of the strategy group is to prepare a strategic assessment in accordance with Regulations 5 to 7 and a partnership plan in accordance with Regulations 10 and 11. The strategic assessment is an analysis of the levels and patterns of crime and disorder and substance misuse in the area and the priorities the CDRP should adopt to address those matters. The partnership plan sets out a strategy for meeting those priorities and how that strategy should be

implemented by the CDRPs. Under Regulation 9 there is a requirement that a county wide group produce a community safety agreement in two tier areas for the county based on the strategic assessments of each area in that county.

The Regulations also include provisions to facilitate information sharing within CDRPs and ensure that when preparing and implementing a strategic assessment and partnership plan the CDRPs engage with their local communities.

Notes:

[1] 1998 c.37; section 6 was substituted by section 22 of, and Schedule 9 to, the Police and Justice Act 2006 (c.48) and is in force from 1st August 2007 (S.I. 2007/1614). There are amendments to section 114 of the 1998 Act not relevant to these Regulations.

[2] Section 5(2) of the 1998 Act has been amended by section 97 of the Police Reform Act 2002 (c.30).

[3] 2006 c.48. Section 19 of the 2006 Act is not yet in force.

[4] Section 5(3) of the 1998 Act has been amended by section 97 of the Police Reform Act 2002.

[5] Section 17A was inserted into the 1998 Act by section 22 of, and Schedule 9 to, the Police and Justice Act 2006 and is in force from 1st August 2007 (S.I. 2007/1614).

[6] Section 115 has been amended by section 74 of, and Schedule 7 to, the Criminal Justice and Court Services Act 2000 (c.43), section 97 of the Police Reform Act 2002, section 219 of the Housing Act 2004 (c.34), section 22 of, and Schedule 9 to, the Police and Justice Act 2006 (those amendments are in force from 1st August 2007 (S.I. 2007/1614)) and by S.I. 2000/90 and S.I.2002/2469.

APPENDIX C, SI 2007 NO, 1831

S T A T U T O R Y I N S T R U M E N T S

2007 No. 1831

CRIMINAL LAW, ENGLAND AND WALES

The Crime and Disorder (Prescribed Information) Regulations 2007

Made

22nd June 2007

Laid before Parliament

29th June 2007

Coming into force

1st August 2007

The Secretary of State, in exercise of the powers conferred by sections 17A(2) and 114(1) and (2) of the Crime and Disorder Act 1998(1), makes the following Regulation:

Citation, commencement and interpretation

1.—(1) These Regulations may be cited as the Crime and Disorder (Prescribed Information) Regulations 2007 and shall come into force on 1st August 2007.

(2) In these Regulations—

“area” means a local government area;

“depersonalised information” means information that does not constitute personal data within the meaning of the Data Protection Act 1998(2);

“general postcode address” means the outward part of the postcode of an address;

“hospital” means a hospital as defined in section 275 of the National Health Service Act 2006(3) that provides services on behalf of a Primary Care Trust or a Local Health Board;

“information period” means each consecutive period of three months beginning on 1st July 2007;

“school” has the meaning given to it in section 4 of the Education Act 1996(4); and

“the 1998 Act ” means the Crime and Disorder Act 1998.

Sharing of Information by Responsible Authorities

2. The information prescribed for the purposes of section 17A of the 1998 Act is depersonalised information of the description specified in the Schedule for the information period.

3.—(1) The interval at which the information of the description specified in the Schedule is to be disclosed is prescribed for the purposes of section 17A of the 1998 Act as by the end of the information period following that to which the information relates.

(2) The first information period within which information shall be disclosed is the period beginning on 1st October 2007.

4. The form prescribed for the purposes of section 17A of the 1998 Act as the form in which the information of the description specified in the Schedule is to be disclosed is electronically.

Scotland of Asthal, Q.C.
Minister of State

Home Office
22nd June 2007

Regulation 2

SCHEDULE Description of Information

1. Information held by the police force for the area on the category of each—

- (a) anti –social behaviour incident,
- (b) transport incident, and
- (c) public safety/welfare incident,

in the area, as defined in accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales for 2007/2008, and the time, date and location of each of those incidents.

2. Information held by the police force for the area on the sub-category of each crime classified as—

- (a) burglary,
- (b) criminal damage,
- (c) drug offences,
- (d) fraud and forgery,
- (e) robbery,
- (f) sexual offences,
- (g) theft and handling stolen goods,
- (h) violence against the person, and
- (i) other offences,

in the area, as defined in accordance with the Home Office Notifiable Offences List as at the date of these Regulations, and the time, date and location of each of those crimes.

3. Information held by the fire and rescue authority for the area on the time, date and location of each—

(a) deliberate primary fire (excluding deliberate primary fires in vehicles) in the area,

(b) deliberate primary fire in vehicles in the area,

(c) deliberate secondary fire (excluding deliberate secondary fires in vehicles) in the area,

(d) incident of violence against employees of the fire and rescue authority in the area, and

(e) fire in a dwelling in the area where no smoke alarm was fitted attended by the fire and rescue services of the authority,

as defined in accordance with Fire Statistics, United Kingdom 2005.

4. Information held by the fire and rescue authority for the area on the time and date of each call to the fire and rescue services in the area in relation to a malicious false alarm and the purported location of those alarms as defined in accordance with Fire Statistics, United Kingdom 2005.

5. Information held by the local authority for the area on the time, date and location of each road traffic collision in the area and the number of adults and children killed, seriously injured and slightly injured in each of those collisions.

6. Information held by the local authority for the area on the age and gender of each of the pupils subject to a permanent or fixed term exclusion from state primary and secondary schools in the area, the names and addresses of the schools from which those pupils have been excluded and the reasons for their exclusion.

7. Information held by the local authority for the area on the time, date and location of racial incidents in the area as defined in accordance with Best Value Performance Indicators: 2005/06 published by the Office of the Deputy Prime Minister.

8. Information held by the local authority for the area on the category, time, date and location of each:—

(a) incident of anti-social behaviour identified by the authority, and

(b) incident of anti-social behaviour reported to the authority by the public,

in the area, as defined in accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales for 2007/2008 or any other system for classifying anti-social behaviour used by that authority as at the date of these Regulations.

9. Information held by each Primary Care Trust or Local Health Board the whole or any part of whose area lies within the area on the general postcode address of persons resident in the area admitted to hospital, the date of such admissions and the sub-categories of each admission within the blocks—

(a) assault (X85-Y09),

(b) mental and behavioural disorders due to psychoactive substance use (F10-F19),

(c) toxic effect of alcohol (T51), and

(d) other entries where there is evidence of alcohol involvement determined by blood alcohol level (Y90) or evidence of alcohol involvement determined by level of intoxication (Y91),

as classified in accordance with the International Classification of Diseases, Tenth Revision (ICD-10) published by the World Health Organisation.

10. Information held by each Primary Care Trust or Local Health Board the whole or any part of whose area lies within the area on the general postcode address of persons resident in the area admitted to hospital in respect of domestic abuse as defined in Section 2.2 of the Responding to domestic abuse: a handbook for health professionals published by the Department of Health in December 2005, and the date of such admissions.

11. Information held by each Primary Care Trust or Local Health Board the whole or any part of whose area lies within the area on the number of —

(a) mental illness outpatient first attendances, and

(b) persons receiving drug treatment,

in the area.

12. Information held by each Primary Care Trust or Local Health Board the whole or any part of whose area lies within the area on the location, time and date of ambulance service calls to incidents relating to crime and disorder and the category of such incidents using any system for classifying crime and disorder used by that authority.

(1)

[1998 \(c.37\)](#); section 17A of the 1998 Act was inserted by section 22 of, and Schedule 9 to, the Police and Justice Act [2006 \(c.48\)](#) and is in force from 1st August 2007 (S.I. 2007/1614). There are amendments to section 114 of the 1998 Act not relevant to these Regulations. [Back \[1\]](#)

(2)

[1998 c. 29](#). [Back \[2\]](#)

(3)

[2006 c.41](#). [Back \[3\]](#)

(4)

[1996 c.56](#). [Back \[4\]](#)

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations, which come into force on 1st August 2007, relate to the duty to share depersonalised information amongst relevant authorities in a local government area under section 17A of the Crime and Disorder Act 1998. Regulation 2 and the Schedule prescribe the description of information to be shared. Regulation 3 prescribes the interval at which such information must be shared as by the end of each three month period following the three month period to which the information must relate. The duty to share will first apply in the three month period beginning on 1st October 2007 in respect of

information for the previous three month period. Regulation 4 prescribes that the information must be shared electronically.

The National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales for 2007/2008 is available from the Home Office at 2 Marsham Street, London SW1P 4DF; the Home Office Notifiable Offences List is available on the website <http://www.homeoffice.gov.uk/rds/countrules.html>; Fire Statistics, United Kingdom 2005 is available on the website <http://www.communities.gov.uk/index.asp?id=1509023>; Best Value Performance Indicators: 2005/06 published by the Office of the Deputy Prime Minister is available on the website <http://www.audit-commission.gov.uk/performance/guidance.asp>; the International Classification of Diseases, Tenth Revision (ICD-10) published by the World Health Organisation is available from the website <http://www.who.int/classifications/apps/icd/icd10online/>. and Responding to domestic abuse: a handbook for health professionals is available on the website http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4126161

Crime and Disorder Act 1998

INTER AGENCY INFORMATION REQUEST AND RESPONSE FORM

Only Designated Officers may request or provide information.

Designated Officers must retain a signed hard copy of the form for audit / disclosure purposes. All information received or provided is subject to the Data Protection Act 1998 and the common law duty of confidentiality.

Information may be requested or provided using a secure email network.

Information must not be used for any purpose other than that for which it is requested and must not be disclosed to an unauthorised person. There must be no secondary disclosure of information without the written consent of the agency that provided the information.

Information must be retained within a secure environment. Retained information should be destroyed as soon as it has served its required purpose or reached its expiry date.

Reference number : (location/ year/ reference number) __/__/__

REQUEST

To: Organisation
 Name
 Address
 Telephone number
 Position in organisation

From : Organisation
 Name
 Address
 Telephone number
 Position in organisation

Please provide details of the person, project, vehicle or address for which information is to be disclosed. Always include current address if known. Also include any known alias, maiden name, date of birth and ethnicity

Name
 Alternative names
 Address
 DOB
 Ethnicity

I am making enquiries regarding the above named subject concerned with: (*delete sections that do not apply*)
 The prevention and detection of crime and disorder
 The apprehension or prosecution of offenders
 The maintenance of community safety
 Other (specify grounds)

Information is sought under the following legislation (indicate which act you are seeking information under)
 Data Protection Act 1996 Crime and Disorder Act 1998

Purpose for Requesting the Information

We are presently (considering) taking the following action:	
The information you provide will be used to/for:	
If information is urgently required (i.e within 2 working days of the request) please specify the reason for the urgency (reasons for urgency <u>must</u> be confirmed by telephoning the recipient of the request for information):	
If information is not disclosed, how will this effect the project or investigation:	
Will the project/ investigation be compromised by seeking the written consent of the subject of enquiry <i>(delete as appropriate)</i> Yes / no	
Data Protection Act Requests only: Consent of Data Subject has been obtained: Yes / No Consent of Data Subject attached: Yes / No	
Target date for destruction / disposal/ return of information to the provider:	
Signed I confirm I am a Designated Officer authorised under the Information Sharing Protocol and that application confirms with the protocol	Position / Rank
Name	Date 2006

The following is for completion by the Data Owner

RESPONSE	
Decision: yes / no What information was disclosed:	
If approval was given in the original request for information, for the consent of the subject to be sought before disclosure, please confirm whether consent has been obtained Yes / No	
Date request received:	Date of Response
Signed I confirm I am a Designated Officer authorised under the Information Sharing Protocol	Position in Organisation
Name	Date 2006

Remember! Incomplete or wrongly completed applications will be returned