CRIME AND DISORDER ACT 1998
AVON AND SOMERSET PARTNERSHIP
INFORMATION EXCHANGE
PROTOCOL FOR CRIME AND DISORDER

1. Parties/Signatories

Chief Constable	Avon and Somerset Constabulary
Clerk to the Police Authority	Avon and Somerset Constabulary
Chief Executives	Avon Health Community :-
	Avon Health Authority
	Bristol North PCG (PCT from April 2002)
	North Somerset PCG (PCT from April 2002)
	South Gloucester PCT
	Bath and North east Somerset PCT
	Bristol and South West PCG (PCT from April 2002)
	Avon and Wiltshire Mental Health Partnership
	Avon Ambulance NHS Trust
	North Bristol NHS Trust
	Royal National Hospital for Rheumatic Diseases
	Royal United Hospital
	United Bristol Healthcare Trust
	Weston Area Health Trust
Chief Executive	Somerset Health Authority (on behalf of the Somerset Health Community)
Chief Executive	National Probation Service for England & Wales (Avon & Somerset region)
Chief Executive	Bath & North East Somerset Council
Chief Executive	Bristol City Council
Chief Executive	Mendip District Council
Chief Executive	North Somerset Council
Chief Executive	Sedgemoor District Council
Chief Executive	Somerset County Council
Chief Executive	South Gloucester Council
Chief Executive	South Somerset District Council
Chief Executive	Taunton Deane Borough Council
Chief Executive	West Somerset District Council

Organisations and agencies in the statutory, voluntary and community sector (or organisations by order of the Secretary of State) may also become signatories to the protocol where this is necessary or expedient to the successful implementation of the Act.

It will be the responsibility of these signatories to ensure that:

- realistic expectations prevail from the outset;
- ethical standards are maintained;
- a mechanism exists by which the flow of information can be controlled;
- appropriate training is provided;
- adequate arrangements exist to test adherence to the protocol.

2. Purpose

The purpose of this protocol is to facilitate the exchange of information in order to comply with the statutory duty on the signatories to work together to develop and implement a strategy and tactics for crime reduction, as required under the Crime and Disorder Act 1998.
This protocol is mainly concerned with the exchange of personal information. Therefore, where de-personalised information is requested the assumption is that this information will be shared. Wherever possible, information that does not identify individuals should be used and disclosed such as aggregated or statistical information.

This protocol does not cover the work of the Youth Offending Teams. It is recognised that other protocols may be developed in the future for specific areas of activity.

3. Introduction

The Avon and Somerset Partnership subscribes to the following for this protocol:

- the agreed standards must provide safeguards and an appropriate framework for the controlled exchange of relevant information;

- the Data Protection principles must be upheld (The principles are outlined at **Appendix A**);

- this protocol to be reviewed annually;

- any partner may request any change to the protocol at any time by submitting to the protocol holder a suggested revision;

- the nominated holder of this protocol is the Force Data Protection and Information Security Manager, Avon and Somerset Constabulary, who shall on behalf of the partnership:

  a) ensure that a review is carried out on an annual basis;

  b) circulate all requests for change, co-ordinate responses, obtain agreement for

the changes from the partnership and distribute codes of practice and guidance as these become available.

4. Definitions

For the purpose of this protocol “crime” is defined as any act, default or conduct prejudicial to the community, the commission of which by law renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.

The term “anti-social behaviour” means acting in a manner which causes or is likely to cause harassment, alarm, or distress to one or more persons who are not of the same household as the identified person.

“Disorder” is an expression that refers to the level or pattern of anti-social behaviour within a particular area.

“Prevention of Offending” is activity which reduces the likelihood of offending/re-offending by promoting peoples best interests through provision of community programmes, that reduces the risk factors associated with offending and promotes protective factors.

“Personal data” is information that relates to a living individual that can be identified from those data, or from those data and other information which is likely to come into the possession of the data controller. It includes any expression of opinion or intentions in respect of the individual.

“De-personalised data” means information where an individual cannot be identified, for example by using information such as the first group and only the 1st character of second group of a post code such as BS20 9--.

“Data controller” means a person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be, processed.

5 Information Exchange

Disclosure of any personal data must be bound to both common and statute law, for example defamation, the common law duty of confidence, the Data Protection Act 1998, and the Human Rights Act 1998.

The data protection principles require that such information is obtained and processed fairly and lawfully; is only disclosed in appropriate circumstances; is accurate, relevant, and not held longer than necessary; and is kept securely.

The Human Rights Act 1998 gives further effect in domestic law to certain Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to read compatibly with the Convention Articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a public authority fail to do this then it may be subject of a legal action under section 7. This obligation should not solely be seen in terms of an obligation not to violate Convention Rights but also as a positive obligation to uphold these rights.

The sharing of information between agencies has the potential to infringe a number of Convention Rights. In particular, Article 3 (Freedom from torture or inhuman or degrading treatment), Article 8 (Right to private and family life), and Article 1 of Protocol 1 (Protection of Property). In addition all Convention Rights must be secured without discrimination on a wide variety of grounds under Article 14 (Prohibition of Discrimination).

The Convention does allow limited interference with certain Convention rights by public authorities under broadly defined circumstances known as legitimate aims. However, mere reliance on a legal power may not alone provide sufficient justification and the following principles should be considered:

- is there a legal basis for the action being taken;
- does it pursue a legitimate aim (as outlined in the particular Convention article);
- is the action taken proportionate and the least intrusive method of achieving that aim;

A brief summary of the Articles of the Human Rights Act 1998 is attached at **Appendix B**. Article 8 is covered in more detail at 5.2 (d) but other articles may apply in specific circumstances.

5.1 Depersonalised Data

Depersonalised data should be used unless the purpose could not be achieved by this means alone.

To undertake the crime audit there is a presumption that management teams and consultative committees do not require personal data. Those involved in the crime audit may receive personal data only if the failure to do so would prevent the achievement of their objectives.

Any personal data exchanged should be protected and secured, by all parties, in accordance with this protocol.

5.2 Personal Data - Power to Disclose

If failure to share personal information means that the purpose of this protocol could not be achieved, each party must carefully consider each of the following prior to making any decision:

a) Section 115 of Crime and Disorder Act 1998

Where the disclosure is necessary or expedient for the purposes of any provision of the Act.

Section 115 ensures all agencies have a power to disclose; it does not impose a requirement on them to exchange information, control remains with the partner that holds the data.

b) Consent

Many of the data protection issues surrounding the disclosure can be avoided if the informed consent of the individual has been sought and obtained. Consent must be freely given after the alternatives and consequences are made clear to the person from whom permission is being sought. If the data is classified as sensitive data the consent must be explicit. In this case the specific detail of the processing should be explained:

- the particular types of data to be processed;
- the purpose of the processing;
- any special aspects of the processing which may affect the individual, e.g. disclosures.

In the absence of consent, the nominated officer must balance the duty of care and the public duty of confidentiality against the need to prevent and detect crime and disorder, and serve the public interest, in order to make a positive decision whether or not to release the information.

No details of victims, witnesses or complainants should be disclosed without their written consent (Swinney v Chief Constable of Northumbria).

c) Public Interest

If informed consent has not been sought, or sought and withheld, the partner must consider if there is an overriding public interest of justification for the disclosure. In making this decision the following should be considered:

- is the disclosure necessary for the prevention or detection of crime, prevention of disorder, to protect public safety, or to protect the freedoms of others;
- is the disclosure necessary for the protection of young or other people;
- what risk to others is posed by this individual;

- what is the vulnerability of those who may be at risk;
- what will be the impact of the disclosure;
- is the disclosure proportionate to the intended aim;
- is there an equally effective but less intrusive alternative means of achieving that aim.
-

d) Human Rights - Article 8

Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law, in particular: -

- public safety;
- the prevention of crime or disorder;
- the protection of health or morals;
- the protection of the rights or freedoms of others.

5.3 Extent of Personal Data Disclosed

Disclosure of personal data must be relevant and the minimum amount required for the purpose.

The identity of the originator must be recorded against the relevant data. No secondary use or other use may be made unless the consent of the disclosing party to that secondary use is sought and granted. Disclosure must be compatible with the second data protection principle: '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'.

5.3.1 Proportionality

The principle of 'proportionality' is a common theme running through both the Convention rights and judgements of the European Court. It is explicitly expressed in the limitations contained in Articles 8 - 11 where it is stated that any interference or restriction of those rights must be lawful and 'necessary in a democratic society'. Any restriction of rights must, therefore, be justified in that a fair balance must be achieved between the protection of an individual's rights with the general interests of society. In the context of information exchange, any disclosure of information should be restricted to a minimum and be the least damaging that is required in achieving the objective.

5.4 Review and Weeding of Data

One of the principles within the data protection legislation states that excessive data must not be retained. It follows that information must be removed as soon as it is no longer required for the original purpose for which it was supplied or collected (principles 3 & 5 apply).

Therefore, retention should be for the minimum period required to achieve the objectives of the disclosure after which the data will be returned to the originator or destroyed as agreed. For example, in connection with an Anti-Social Behaviour Order the only information to be retained should be the date and conditions, all other data should be weeded when the order is obtained and the appeal period expired.

5.5 Data Quality

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

5.6 Designated Officers

Each partner (signatories) to this protocol must designate someone within their organisation to assume responsibility for data protection (including notification if appropriate); security and confidentiality; and compliance with legislation, e.g. by undertaking audits. If notification is required, the disclosure to cover information sharing within these partnerships should be worded as follows: "Relevant authorities as defined in Section 115 of the Crime and Disorder Act 1998, in the context of Crime and Disorder legislation".

5.7 Requesting /disclosing personal information.

Disclosures and requests for disclosures must be in writing, using the forms at **Appendix D**, and retained. Decisions on disclosures reached at meetings must be minuted.

Each partner shall complete (and thereafter maintain) **Appendix E** and submit to the nominated protocol holder for circulation to all other partners, a list of key staff:

- to whom requests for information should be sent;
- to whom disclosures should be made;
- with whom contact should be made in relation to this protocol;
- who are responsible for data protection and security.

Requests from unauthorised organisations/staff will be declined. Disclosure of information from Health and Social Services must be endorsed by the relevant Caldicott Guardian. The principles of the Caldicott Guardians are attached at **Appendix C.**

This information will provide evidence if the disclosure is challenged or formal complaint is made. Clear records of the evidence provided by various partners will be required to justify any challenges of the proportionality of the action taken. Care should be taken when any request for disclosure emanates from private, commercial or unprecedented sources, in which, case reference must be made to designated Data Protection Officers.

5.7.1 Case Conferences

Case conferences may be held when deemed necessary by all partners. Information exchanged at such a meeting will be minuted and given in accordance with the confidentiality agreement at **Appendix F**, which must be noted by all present prior to the commencement of the meeting.

6. Security

All partners must ensure that a baseline level of security is in place to ensure compliance with principle 7 of the Data Protection Act. The security standard must be compatible with ISO 17799/BS 7799.

7. Complaints and Breaches

Any complaint made will be brought to the attention of the nominated officer of the relevant partner(s), and they will be dealt with in accordance with their own policies and procedures. Partners will keep each other informed of developments following a complaint received, where relevant.

8. Requests for Information

8.1 Subject Access Requests

All requests for information under the subject access provisions of the Data Protection Act 1998 will be dealt with by the person responsible for Data Protection within the organisation. If personal data is identified as belonging to another partner, it will be the responsibility of the receiving partner to contact the Data Protection Officer for the originating partner to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act.

Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless:

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

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

- any duty of confidentiality owed to the other individual;
- any steps taken by the data controller with a view to seeking the consent of the other individual;

- whether the other individual is capable of giving consent;
- any express refusal of consent by the other individual.

8.2 Freedom of Information

Requests for personal information under the Freedom of Information Act, will be dealt with under the amended 'subject access' provisions of the Data Protection Act.

Partners are reminded that these agreements should be publicly available.

9. Training

Each partner is responsible for ensuring that appropriate members of staff are adequately trained in respect of all matters covered in this protocol.

10. Indemnity

Each partner shall be fully indemnified by the other partners in accordance with the indemnity contained in **Appendix G**.

11. Confidentiality

Each partner shall at all times keep confidential all personal data supplied pursuant to this agreement. This clause shall survive termination of the agreement or the withdrawal of or removal of any partner. This means that no publication of data supplied pursuant to this agreement will identify any individual.

12. Signatures

By signing this document the participants accept and will adopt the statements included in this protocol and the indemnity, and agree to maintain the specified standards. In addition, the partners will not use, release or otherwise disclose any information whatsoever:

- for any other secondary use not specified by the Crime and Disorder Act 1998 or by regulations made thereunder; and/or

- to any organisation which is not a signatory to this protocol.

Signed on behalf of: -

Name of organisation and address;

Position/Job title;

Signature;

Dated this [ ] day of [ ] 2002

Appendix A

DATA PROTECTION ACT 1998

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

- at least one of the conditions in Schedule 2 is met and;
- in the case of sensitive data at least one of the conditions in Schedule 3 is also met.

Principle 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.

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Principle 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.

Principle 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 freedom of data subjects in relation to the processing of personal data.

Appendix B

HUMAN RIGHTS

Article 2 - Right To Life

Everyone's right to life shall be protected by law

Article 3 - Prohibition of Torture, Inhuman or Degrading Treatment

No one shall be subjected to torture or to inhuman or degrading treatment or punishment.

Article 4 - Prohibition of Slavery and Forced Labour

No one shall be held in slavery or servitude.

No one shall be required to perform forced or compulsory labour.

Article 5 - Right to Liberty and Security

Everyone has the right to liberty and security of person.

Article 6 - Right to a Fair Trial

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.

Article 7 - No Punishment Without Law

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.

Article 8 - Right to Respect for Private and Family Life

Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law.

Article 9 - Freedom of Thought Conscience and Religion

Everyone has the right to freedom of thought, conscience and religion;

Article 10 - Freedom of Expression

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

Article 11 - Freedom of Assembly

Everyone has the right to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.

Article 12 Right to Marry

Men and Women of marriageable age have the right to marry and to found a family, according to their national laws governing the exercise of this right.

Article 14 - Prohibition of Discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Article 16 Restriction on the Political Activity of Aliens

Nothing in articles 10,11 and 14 shall be regarded as preventing the High Contracting Parties from imposing restrictions on the political activity of aliens.

Article 17 - Prohibition of Abuse of Rights

Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.

Article 18-Limitation on use of Restrictions on Rights

The restrictions permitted render this Convention to tire-said rights and freedoms shall not be applied for any purpose other than those for which they have been prescribed.

The First Protocol

Article 1 - Protection of Property

Every natural or legal person is entitled to the peaceful enjoyment of his possessions.

Article 2 - Right to Education (subject to UK reservation)

No person shall be denied the right to education.

Article 3 - Right to Free Elections

The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot

The Sixth Protocol

Article 1 - Abolition of Death Penalty

The death penalty shall be abolished. No one shall be condemned to such penalty or executed.

Article 2 - Death penalty in Time of War

A State may make provision in its law for the death penalty in respect of acts committed in time of war or imminent threat of war.

Appendix C

CALDICOTT GUARDIAN PRINCIPLES

- **That the purposes for using patient information need to be justified**
- **Patient identifiable information to be used only when absolutely necessary**
- **The minimum patient identifiable information to be disclosed**
- **Access should be restricted on that basis**
- **That all those disclosing information should be aware of their responsibilities and everyone who is involved should understand and comply with the law**

Appendix D

Name of partner organisation:

Crime and Disorder Act 1998

Data Protection Act

Disclosure of Personal Data

To:	Your Reference:

Further to your written request dated …… the information you have asked for about (Full Name)……

is as follows:

(Grounds for Disclosure shown overleaf – Section 1 must be completed)

Signed:		Date:	
Name:		Rank/Job Title:	

You are reminded that this information is supplied on the following basis;

(i) the data must be used for the specific purpose for which it was requested and disclosed;
(ii) the data must be retained securely and in accordance with the standards included in the protocol;
(iii) you will destroy the data when it ceases to be required for the specific purpose for which it was requested and disclosed.

Grounds for Disclosure

Section 1 – Full explanation as to why the public interest outweighs the duty of confidentiality:

Section 2 – Required for:	**Tick**
The prevention of crime	
The detection of crime	
The prosecution of offenders	

Note: Section 2 should be completed if possible.

Name of partner organisation:

Crime and Disorder Act 1998

Data Protection Act

Request for Personal Data

I am making enquiries into matters covered by the Crime and Disorder Act 1998 and require personal information about: -

Full Name:

Date of Birth:

Place of Birth:

Thought to be living at:

Male/Female

The Information I require is: -

I confirm that the personal data requested is required for the purpose indicated overleaf and failure to provide information will, in my view, be likely to directly prejudice that purpose.

Signed:		Date:	
Name (Capitals):		Rank/Job Title:	

Activity	Tick
Prevention of Crime and Disorder	
Detection of Crime	
Reduction of Crime and Disorder	
Crime displacement	
Tackling crime on housing estates	
Street crime activity	
Truancy/Youth crime	
Maintain public safety	
Public safety – offences under Mental Health Act	
Anti-social behaviour	
Apprehension of offenders	
Diverting young offenders	
Protection of vulnerable members of the community	
Relocation of recently released prisoners to safer residences	

OR

Other activity taken under specific Order
(specify Order)

.....

.....

.....

Appendix E

Name of Partner organisation:

Crime and Disorder Act 1998

Protocol for Data Sharing

The Partner:	

Requests documents to be sent to: (Note: Specify individual departments if necessary)	**Disclosures to be made to:**	**Responsibility for Data Protection and Security**

Dated:

Appendix F

Confidentiality Statement

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality, all attendees are asked to agree to the following.

This agreement will be recorded in the minutes.

1 Information can be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.

2 A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the individuals confidentiality and a breach of the confidentiality of the partners involved.

3 All documents exchanged should be marked 'confidential – not to be disclosed without consent'. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.

4 If further action is identified, the partner(s) who will proceed with this action(s) should then make formal requests to any other partners holding such personal information as may be required to progress this action, quoting their legal basis for requesting such information. Information exchanged during the course of this meeting must not be used for such action.

5 If the consent to disclose is felt to be urgent, permission should be sought from the Chair of the meeting and a decision will be made on the lawfulness of the disclosure such as the prevention or detection of crime, apprehension or prosecution of offenders, or where it is required to prevent injury or damage to the health of any person.

Appendix G

FORM OF INDEMNITY

1. In consideration of the provision of information in accordance with (insert details of agreement or arrangement under which information is to be supported, and insert name of authority granting indemnity) undertakes to indemnify any of the persons or any authority referred to in paragraph 2 below against any liability which may be incurred by such person or authority as a result of the provision of such information.

Provided that this indemnity shall not apply:

(a) where the liability arises from information supplied which is shown to have been incomplete or incorrect, unless the person or authority claiming the benefit of this indemnity establishes that the error did not result from any wilful wrongdoing or negligence on its part or on the part of any other person or authority referred to in paragraph 2 below;

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

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

2. Persons who may claim the benefit of this indemnity are as follows:
   (a) any police authority;
   (b) any chief officer of police;
   (a) any serving or former member of a police force;
   (d) any serving or former civilian of a police authority;
   (e) the National Identification Bureau;
   (f) any local authority;
   (g) any employee or former employee of a local authority;
   (h) any probation authority;
   (i) any employee or former employee of a probation authority;
   (j) any health authority, NHS trust, primary care groups and trusts;
   (k) any employee or former employee of a health authority, NHS trust, primary care groups and trusts;

and in this paragraph the expressions "police authority", "chief officer of police" and "police force" have the same meaning as in section 101 of the Police Act 1996.