Devon & Cornwall Police
Building safer communities together

Protocol for the Exchange of Information between Statutory Agencies in Devon and Cornwall in Relation to Potentially Dangerous or Mentally Disordered Persons

Version 1.0 - Working Version

April 2010

Contents

Protocol for the Exchange of Information between Statutory Agencies in Devon and Cornwall in Relation to Potentially Dangerous or Mentally Disordered Persons

1. Parties/Signatories

1.1 The Signatories to this Protocol are:

1.1.1 Devon & Cornwall Police
1.1.2 Cornwall Council
1.1.3 Cornwall Partnership NHS FoundationTrust
1.1.4 Devon County Council
1.1.5 Devon Partnership NHS Trust
1.1.6 The Council for the Isles of Scilly
1.1.7 Plymouth City Council
1.1.8 NHS Plymouth - Plymouth Primary Care Trust
1.1.9 Torbay Council

1.2 Nominated Persons who are to be the point(s) of contact in respect of each of the Signatories for the purposes of this Protocol are identified in Appendix 3.

2. Background

2.1 The majority of the signatories to this Protocol are parties to the Crime and Disorder Information Sharing Protocol entered into by the signatories and other parties on 1st March 2003.

2.2 The purpose of the Crime and Disorder Information Sharing Protocol is to facilitate the exchange of information (including personal data) between the parties to that Protocol in furtherance of the compliance of relevant parties with the statutory duty imposed on them by Section 17 of the Crime and Disorder Act 1998 to exercise their functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that they reasonably can, to prevent crime and disorder.

2.3 The Crime and Disorder Information Sharing Protocol acknowledges that further information sharing protocols, ancillary to the Crime and Disorder Protocol (termed in the Crime and Disorder Information Sharing Protocol 'Ancillary Protocols'), will be required to cover information exchange in relation to specific areas of work. This Protocol is one such ancillary protocol.

3. Purpose

3.1 The purpose of this Protocol is to support and facilitate the exchange of information (including personal data) between the above signatories to allow them to work together for the purposes of the protection of the public, the prevention of offending, and the detection of crime and prevention of anti-social behaviour by potentially dangerous persons OR persons suffering from a mental disorder.
N.B. The fact that a person is considered as potentially dangerous does not automatically imply that they have mental health issues, or that people with a mental disorder are potentially dangerous.

3.1.1 In furtherance of their compliance with the statutory duty imposed on relevant authorities by Section 17 of the Crime and Disorder Act 1998, to exercise their

functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that they reasonably can, to prevent crime and disorder; and, more particularly:

3.1.2 to enable them to provide assistance to individuals deemed as potentially dangerous, who are or who have a mental disorder who are:

- at risk of committing a crime;
- are suspected of or who have committed offences; or
- who may compromise the safety of themselves or others;

3.1.3 to provide a method of exchanging information promptly that cannot await disclosure at a scheduled meeting.

3.2 It is recognised that such information exchange may act as a catalyst for an arrest or to assist treatment following an arrest when the relevant individual deemed as potentially dangerous or suffering from a mental disorder is taken into custody. It may also guide clinical staff in reporting to the Mental Health Tribunal in the case of detained patients and facilitate the safe delivery of mental health care.

4. Definitions and Interpretation

4.1 All defined terms used throughout this Protocol are described in the Glossary contained at Part I of Appendix 2 to this Protocol.

4.2 This Protocol shall be interpreted in accordance with all and any rules of interpretation set out in Part II of Appendix 2 to this Protocol.

5. Core Objectives, Standards And Legal Powers

5.1 The signatories when preparing this Protocol subscribe to the core objectives and standards utilising the legislation as set out In Appendix 1.

6. Law Governing and Enabling the Exchange of Personal Data under this Protocol

6.1 Each of the signatories acknowledges that it alone is responsible for ensuring and satisfying itself that it is permitted by law to disclose personal data to another signatory in accordance with this Protocol.

6.2 Each of the signatories acknowledges that it alone is responsible for ensuring and satisfying itself that it is permitted by law to receive all and any disclosures of personal data from another signatory in accordance with this Protocol.

6.3 For the avoidance of doubt, acceptance of personal data by a signatory from another signatory shall not be taken to be confirmation of the legality of the disclosure.

7. Legality of Disclosures

7.1 See Appendix 1

8. Procedures for Disclosing Data

8.1 Procedures in Appendix 4

The signatories shall follow the procedures set out in Appendix 4 when requesting and making disclosures and shall be mindful of the restrictions on disclosures detailed in Appendix 7.

8.2 Caldicott

The signatories also acknowledge that the Devon Partnership NHS Trust, the Cornwall Partnership NHS Foundation Trust and the Social Services Departments of Devon County Council, Cornwall Council Plymouth City Council and Torbay Council respectively each have their own procedures governing the release of information to third parties, which have been developed as part of the Caldicott arrangements and that signatories may be required to comply with these. These signatories shall notify the Nominated Holder of all and any such procedures which they expect signatories requesting a disclosure to comply with and the nominated holder shall circulate details of the same to the signatories.

8.3 Compliance with law, this Protocol and internal policies

Each signatory shall be responsible for ensuring that it complies with all relevant legislation and laws, this Protocol, its own internal procedures and policies, and the relevant policies of any professional and / or regulatory bodies which govern the work of the signatory when making a disclosure. To this end, each signatory shall obtain its own legal advice where necessary.

8.4 Minimum Disclosure Necessary

The signatories agree that they will adhere to the principle that any disclosure requested or made should be restricted to the minimum amount of personal data necessary to achieve the purpose of the disclosure and, where appropriate, be as generalised as possible. This will be determined on a case by case basis.

8.5 Proportionality

The signatories agree that if a disclosure will in some way restrict the rights of the relevant data subject the relevant signatory or signatories (as may be appropriate) will consider the rule of proportionality. This is to ensure that a fair balance is achieved between the protection of the data subject's rights and the general interests of society.

8.6 Disclosable Personal Data

Each signatories shall issue guidance to the other signatories through the nominated holder on what types of records containing personal data may potentially be the subject of a disclosure request under this Protocol if they feel that this would be helpful to the other signatories. Details of guidance issued at the date hereof is set out in Appendix 9.

9. Nominated Officers

9.1 For the purposes of maintaining the security of personal data, each of the signatories shall nominate a member (or members) of their staff who shall act as a nominated officer (or nominated officers) who shall be the point(s) of contact for that signatory for the purposes of matters concerning this Protocol. The nominated officers nominated at the date hereof are identified in Appendix 3.

9.2 The relevant nominated officers shall be the only point of contact for each signatory for (without limitation):

9.2.1 The nominated officer is the single point of contact for any other signatory requesting a disclosure or any other request for relevant information from it; and

9.2.2 To whom Disclosures should be made.

9.3 Any change in a nominated officer will be notified to the nominated holder, in writing, by the relevant signatory. The nominated holder shall then inform all other signatories of the change made.

9.4 The list of named nominated officers within Appendix 3 in considered Restricted Data and not disclosable under the Freedom of Information Act 2000. Therefore, this section of the document should not be transmitted over any insecure internet link.

10. Registration/Notification under the DPA 1998

10.1 Each signatory will ensure that it is appropriately registered under the DPA 1998 at all times to receive, disclose and otherwise process personal data in accordance with the provisions of this Protocol.

11. Compliance with the DPA 1998

11.1 Each of the signatories shall ensure that it complies with the DPA 1998 at all times in respect of its processing of personal data which is the subject of this Protocol.

11.2 Without prejudice to Clause 12.1, each signatory shall ensure that it complies with the First Data Protection Principle, set out in Schedule 1 of the DPA 1998, when obtaining and otherwise processing personal data which is the subject of this Protocol unless for any reason stated in the DPA 1998 or other relevant legislation such compliance is not required or only partial compliance is required.

12. Accuracy of Data

12.1 The signatories acknowledge that they each have a responsibility to verify and maintain the accuracy of personal data held by them which is subject to this Protocol, this being a statutory duty set out in Schedule 1 of the DPA 1998.

12.2 Where an inaccuracy is discovered, after a disclosure has been made, it will be the responsibility of the signatory discovering the inaccuracy to bring this to the notice of the signatory making the disclosure, in writing, who will notify all other signatories who have also received the same personal data from it of the inaccuracy and any correction required in respect of that inaccuracy.

12.3 In order to meet the obligations under Clause 12.2, signatories are expected to record disclosures made.

13. Data Standards

13.1 The signatories acknowledge that the national standard for making data (including personal data) 'fit for use' is industry standard BS7666. The signatories recognise the benefits that might be brought to the disclosure process and other information sharing carried out under this Protocol by the processing of data which they hold in accordance with this standard BS7666. To this end the signatories will endeavor to adopt this standard in respect of such processing to the extent that this accords with their respective internal policies and procedures in this regard.

14. Use of Personal Data and Privacy

14.1 Process in accordance with purpose

The signatories shall only use and otherwise process any personal data received by means of a disclosure in accordance with the purpose of this agreement and any specific purpose identified on a 'Request for Disclosure Form' submitted in accordance with the procedures set out in Appendix 4.

14.2 Disclosure of personal data to another signatory

For the avoidance of doubt, a signatory which received personal data through a disclosure made by another signatory shall not disclose such personal data to a different signatory without the consent of the signatory which made the original disclosure.

14.3 This clause 12 shall survive termination of the Protocol or the withdrawal of or removal of any signatory.

15. Security

15.1 Each signatory shall at all times maintain privacy controls for all personal data supplied pursuant to this Protocol.

15.2 The signatories will use the established appropriate Government Protective Marking System for all data transfers.

15.3 Each signatory will take all reasonable steps to adequately protect the personal data received by it from another signatory from both a technological and physical point of view from unauthorised or unlawful processing of the personal data and accidental loss or destruction of, or damage to, the personal data.

15.4 The Devon & Cornwall Police will grade the personal data provided to them, to restrict access, where this is applicable.

15.5. Without prejudice to Clause 15.1, each signatory shall ensure that access to personal data and other information obtained from another signatory pursuant to and / or in accordance with this Protocol by individuals employed or otherwise engaged by that signatory shall be restricted to those individuals who require such access.

15.6. The signatories recognise the merit of maintaining a full audit record of all disclosures made to them.

15.7. The signatories acknowledge that the national standard for making data (including personal data) secure is industry standard ISO/IEC 27000. The signatories will endeavour to adopt this standard in respect of all processing of personal data, de-personalised data and other data which they carry out as a result of this Protocol insofar as this accords with their respective internal policies and procedures in this regard.

15.8. The provisions of this Clause 12 will survive termination of the Protocol or the withdrawal of or removal of any signatory.

16. Agents, Contractors and Service Partners

16.1 Whereas the Data Protection Act 1998 permits the sharing of personal data between signatories to the Protocol it is recognised that the signatories may wish and / or need to engage a third party data processor to process all and / or any personal data received through a disclosure. When making a release of such personal data to a third party data processor the relevant signatory shall:

16.1.1 ensure that an appropriate written contract is put in place between the signatory and the data processor which makes provision for and controls the processing to be carried out by the data processor and which provides that the data processor is act only on the instructions of the relevant signatory;

16.1.2 obtain from the data processor sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out;

16.1.3 ensure that it retains and / or obtains sufficient access rights to enable it to confirm that such guarantees are being complied with, to respond to any complaints and breaches made in respect of any processing and to satisfy Subject Access Requests (see Appendix 10).

16.1.4 take reasonable steps to ensure that the data processor complies with any such guarantees;

16.1.5 take measures to ensure that the data processor does not transfer the personal data to a third party; and

16.1.6 inform any other signatory from whom it obtained any of the relevant personal data that the processing is to be carried out by the data processor.

17. Subject Access Requests

17.1 See Appendix 10

18. Complaints

18.1 Any and all complaints made in respect of disclosures or other matters relating to this Protocol or addressed in this Protocol will be brought to the attention of the nominated officer of the relevant signatories by the signatory receiving the complaint, and they will be dealt with in accordance with the relevant internal policies and procedures of the relevant signatories.

18.2. Signatories will keep each other informed of developments following a complaint received, where relevant.

19. Compliance and Good Practice

19.1 Any further guidance or Codes of Practice should be reviewed annually and distributed via the nominated holder for consideration and possible attachment to this Protocol.

20. Changes to the Protocol

20.1 All and any signatories may request any change to the Protocol at any time by submitting a request to the nominated holder.

20.2 Upon receipt of any requests for changes to the Protocol the nominated holder shall:

20.2.1 circulate the requests to all the signatories;

20.2.2 co-ordinate responses received from any signatories to the same; and

20.2.3 where appropriate, seek the agreement to the requested changes from the signatories.

20.3 No change shall be made to the Protocol except with the agreement of all of the signatories, which agreement shall be recorded in writing.

20.4 A memorandum of any changes to this Protocol agreed by the signatories from time to time shall be endorsed upon this Protocol and the nominated holder shall be responsible for arranging the same.

21. Regular Review of Protocol and Consultation Regarding Protocol

21.1 Any further guidance or codes of practice should be reviewed annually and distributed via the nominated holder for consideration and possible attachment to this Protocol.

21.2 The nominated holder shall ensure that a review of the Protocol is carried out by the signatories:

21.2.1 within the first six (6) months of the date of the Protocol being signed;

21.2.2 on an annual basis; and

21.2.3 in the event that any new legislation comes into force or official guidance is issued which impacts on the Protocol or the obligations of all or any of the signatories under the Protocol.

21.3 The signatories shall consult with each other regarding matters of policy and strategy which directly arise from or in any way impact on this Protocol.

22. Changes to Signatories

22.1 Withdrawal / Removal of Signatory from Protocol

Any signatory may withdraw from being a signatory to this Protocol upon giving written notice to the other signatories.

22.2 In the event that a signatory materially breaches a term of this Protocol or persistently breaches the terms of this Protocol the other signatories may upon a majority vote where each signatory other than the signatory in breach has one vote remove that signatory's status as a signatory of this Protocol provided that all of the other signatories submit their vote.

22.3 The Signatories will do all acts and enter into all such documents as are necessary to give legal effect to the withdrawal or removal of a Signatory pursuant to Clauses 23.1 or 23.2.

22.4 All personal data received by means of disclosures from other signatories must be returned or destroyed at the reasonable request of those signatories in the event of a signatory withdrawing from or being removed from this Protocol.

22.5 Any signatory who withdraws or is removed from this Protocol must continue to comply with the terms of this Protocol in respect of any information (including personal data) that the signatory has received as a result of being a signatory to this Protocol.

22.6 Additional Signatories

Third parties may also become signatories to the Protocol where this is necessary or expedient to the successful implementation of the purpose or necessary expedient to that third party's compliance with any statutory duty imposed on it by Section 17 of the Crime and Disorder Act 1998.

22.7 The signatories shall do all acts and enter into all such documents as are reasonably necessary to give legal effect to a third party, becoming a party to this Protocol where appropriate.

23. Indemnity

23.1 Subject to Clauses 23.2 and 23.3, in consideration of the agreement to make disclosures of personal data in accordance with this Protocol each of the signatories (each an 'Indemnifying Signatory') shall indemnify each and all of the other signatories and keep

each and all of the other signatories fully and effectively indemnified against all direct losses, claims, damages, liabilities (whether criminal or civil), costs, charges, expenses (including without limitation, legal fees and costs), demands, proceedings and actions which all or any of the other signatories may incur or which may be brought about or established against them by any person and which in any case arises out of or in relation to or by reason of:

23.1.1 any breach by the indemnifying signatory, its servants or agents, of any of the provisions of this Protocol;

23.1.2 without limitation to Clause 23.1.1 any processing by the Indemnifying signatory, its servants or agents, of personal data received by reason of a disclosure for purposes other than the Purpose; or

23.1.3 any breach by the indemnifying signatory, his servants or agents, of any law in respect of its processing of personal data received by reason of a disclosure made by another signatory.

23.2 The indemnity set out in Clause 23.1 shall not apply where such direct losses, claims, damages, costs, charges, expenses, liabilities, demands, proceedings and actions are accrued solely as a result of the wrongful acts or omissions of the signatory seeking to enforce the indemnity.

23.3 In the event of any third party action, claim or demand (the 'Claim'), the indemnity set out in Clause 23.1 shall only apply where the signatory claiming the benefit of the indemnity:

23.3.1. has notified the indemnifying signatory against whom it intends to invoke the indemnity within thirty (30) days of receipt of the claim;

23.3.2 consults with that Indemnifying signatory as to how it should proceed with the claim;

23.3.3 neither has made nor makes any admission which may reasonably be prejudicial to the defence of the claim; and

23.3.4 in the absence of contrary agreement with the indemnifying signatory, resists the claim as far as final judgment.

23.4 In the event of any claim being paid or compromised or in the event of final judgment being given against the relevant signatory, the indemnifying signatory shall within fourteen (14) days of being so notified by the relevant signatory pay to that signatory all monies owing to the signatory pursuant to this Clause 24 provided always that where any claim is paid or compromised the Indemnifying signatory shall have the right to be consulted as to the extent of any payment prior to such payment being made.

23.5 Each signatory shall be under a duty to mitigate against all losses which it may incur and in respect of which it makes or intends to invoke the indemnity set out in Clause 23.1.

24. Publication of Protocol

24.1 Subject to Clause 24.2 this Protocol may be published by each of the signatories in accordance with their respective obligations under the Freedom of Information Act 2000.

24.2 No Signatory may publish:

24.2.1 Personal Names and Telephone numbers as part of Appendix 3 to this Protocol; or any other part of the Protocol which the signatories agree from time would, if published, compromise the security of any personal data subject to the Protocol or prejudice the Purpose.

25. Race Relations (Amendment) Act 2000 Impact Statement

25.1 The assessment of the relevance and impact of this Protocol in relation to each Signatory's general duties under the Race Relations (Amendment) Act 2000 is the responsibility of each of the individual signatories.

26. Third Party Rights

26.1 A person who is not a signatory to this Protocol has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Protocol.

27. Counterparts

27.1 This Protocol may be entered into in any number of counterparts and by the signatories to it in separate counterparts, each of which when so executed and delivered shall be an original.

28. Certification

28.1 Protocol for the Exchange of Information Between Statutory Agencies in Devon and Cornwall in Relation to Potentially Dangerous or Mentally Disordered Persons

28.2 By signing below, the signatories accept and agree to be bound by the provisions contained in this Protocol.

Signed: ……ACC Operations.

Name of signatory: Debbie Simpson……..

For and on behalf of Devon and Cornwall Constabulary

Date:

29. Revision Information

Version No	Date of Version
Working Version 1.0 April 2010	Created in 2009/10 due to the need to encompass information sharing linked to Potentially Dangerous Persons, who fell outside the MAPPA process, following a series of inter-agency meeting held in 2009.
January 2011	Additional Contact Officers added for Devon Partnership Trust.

Appendix 1: Core Objectives and Standards and Legal Powers

1.1 The signatories when preparing this Protocol subscribe to the core objectives and standards set out In Appendix 1 in Clause 1.3 and the signatories agree that all amendments to the Protocol agreed by the signatories from time to time pursuant to Clause 22 shall subscribe to the same.

1.2. The signatories agree that this Protocol shall comply with the core objectives and standards set out in clause 1.3.

2.1. The core objectives and standards referred to in Clauses 1.1 and 1.2 are:

2.1.1 the protocol must provide safeguards and an appropriate framework for the controlled and timely exchange of accurate personal data relating to the relevant data subjects;

2.1.2 the Protocol must set out the legal basis for the exchange of the information covered by the Protocol (see below);

2.1.3 in respect of all exchanges of information the DPA 1998 and, in particular, the Data Protection Principles set out in Schedule 1 of the DPA 1998 should be upheld;

2.1.4 the common law principles of confidentiality should be upheld;

2.1.5 the rights of the data subjects and other individuals under The Human Rights Act 1998 should be upheld;

2.1.6 the protocol should be reviewed on a regular basis and in the light of new legislation and/or official guidance; and

2.1.7 any signatory to the protocol may request any change to the protocol at any time and all such requests shall be considered by all of the signatories.

3. Law Governing and Enabling the Exchange of Personal Data Under this Protocol

3.1 Legal Power to Make Disclosures

The Signatories recognise that they may each only make Disclosures insofar as they are legally empowered to do so. In particular, in each case one or more of the conditions set out in Schedule 2 of the DPA 1998 (and in respect of Sensitive Personal Data, one of the conditions set out in Schedule 3 of the DPA 1998 also) must be met.

3.2 Data Protection Act 1998

The signatories acknowledge that they are legally empowered to make Disclosures by any of the following sections of the DPA 1998 Provided that the conditions of those sections are met:

3.2.1 Section 29 (for the prevention or detection of crime, the apprehension or prosecution of offenders, and taxation purposes, and where failure to disclose would be likely to cause prejudice to those purposes);

3.2.2 Section 34 (where information is to be made available to the public by or under enactment);

3.2.3 Section 35 (where the disclosure is required by law or by the order of a court or is made in connection with legal proceedings, for the purpose of obtaining legal advice, and establishing, exercising or defending legal rights);

3.2.4 Section 28 (for the purpose of safeguarding national security);

3.2.5 Section 38 (by order of the Secretary of State).

This list is not intended to be exhaustive. Explanations of the content of the sections shown in brackets are not intended to be full descriptions of the content of the sections and should not be relied on. Signatories shall each be responsible for taking appropriate advice on the application of any such sections in the event that they intend to rely on the same when making a disclosure.

3.3 Crime and Disorder Act 1998 Section 115

Where certain conditions are satisfied, Section 115 of the Crime and Disorder Act 1998 enables any person to disclose information (including personal data) where that disclosure is necessary or expedient for the purposes of any provision of the Crime and Disorder Act 1998 to a relevant authority or to a person acting on behalf of such a Relevant Authority.

3.4 The signatories acknowledge that Section 115 of the Crime and Disorder Act 1998 will enable them to make disclosures to those signatories which are relevant authorities, or who are acting as authorised agents of the relevant authorities in respect of the relevant disclosure, but that Section 115 of that Act does not in itself place a signatory under a statutory duty to make a disclosure to a Relevant Authority or their agent.

3.5 Consent

Disclosures may be made if the consent of the data subject has been obtained or the disclosure is made at the request of the data subject. However, the consent of the data subject may not be possible in the majority of the situations in which the exchange of information empowered by this protocol is activated.

3.6 The protocol partners responsibility for the public protection will at times clash with the responsibility of confidentiality to the individual. Risks to the safety of the individual or others – including members of the public and staff – require prompt action and in such circumstances the presumption of confidentially can be set aside if there is a compelling reason of overriding public interest. Similarly, such action can be taken, in the best interests of the data subject (i.e. where there is no public interest), under a Court Order or under a statutory obligation to disclose information. Prior to disclosure the nominated officer must consider, whether the personal information is held under a duty of confidence, and whether there is an overriding public interest or other justification for disclosing the information, thereby treating the disclosure of information as an exception to the general principals of confidentiality. This will apply even where the individual has refused to allow information to be shared. However, each disclosure must be treated on a case by case basis.

3.7. Data Protection Act 1998, Human Rights Act 1998, Common Law Duty of Confidence

The signatories acknowledge that the legal powers to exchange information described in Clauses 5.1 to 5.5 inclusive above do not override other legal obligations on the signatories in respect of the disclosure and exchange of personal data and, more particularly, those set out in and/or ascribed to:

3.7.1 The Data Protection Act 1998;

3.7.2 The Human Rights Act 1998; and

3.7.3 the common law duty of confidence.

3.8 The signatories shall each take into account and comply with the requirements of the legal obligations on each of them described in Clause 3.1.

3.9 In the case of personal data held under a duty of confidence a disclosure may be made in

respect of that personal data if there is a compelling reason of overriding public interest or another overriding statutory justification which permits the disclosure.

3.10 For the purposes of Clause 3.8 the signatories understand the public interest criteria to include (but not be limited to):

3.10.1 protection of the vital interests of the data subject

3.10.2 the protection of vulnerable members of the community;

3.10.3 maintaining public safety;

3.10.4 the apprehension of offenders;

3.10.5 the prevention of crime and disorder;

3.10.6 the detection of crime; and

3.10.7 the administration of justice.

3.11. The signatories agree to consider the following points when deciding if the public interest criteria should override any duty of confidentiality:

3.11.1 Is the intended disclosure proportionate to the intended aim?

3.11.2 What is the vulnerability of those who are at risk?

3.11.3 What is the impact of the disclosure likely to be on the offender?

3.11.4 Is there another equally effective means of achieving the same aim?

3.11.5 Is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?

3.11.6 Is the disclosure necessary to protect the public?

3.12 The signatories recognise that Article 8 of the Human Rights Act 1998 states that everyone has the right to respect for his private and family life, home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law and is necessary in a democratic society in the interests of:

3.12.1 safety;

3.12.2 economic well being of the country;

3.12.3 the prevention of crime and disorder;

3.12.4 the protection of health and morals; or

3.12.5 the protection of the rights or freedoms of others

and shall apply the same when considering and / or making any disclosures.

3.12 The signatories will comply with all relevant guidance issued by the Home Office and other Government Departments pursuant to or in respect of the Acts or laws referred to in this clause from time to time that, in the event of any conflict between such guidance and the relevant Act(s) or laws then the Act(s) or laws (as may be appropriate) will prevail.

3.14. The Code of Practice on the Management of Police Information

This code was enacted in November 2005 under Section 39 and 39a of the Police Act 1996 and Sections 28, 28a, 73 and 73a of the Police Act 1997. The code sets out principles governing the management of police information, including procedures governing authorised sharing of information obtained and recorded for policing purposes within the police service, and with other agencies. A full Manual of Guidance on the Management of Police Information supporting the requirements of the code was published in March 2006.

3.15 Policing purposes are defined within the code as:

a) protecting life and property;

b) preserving order;

c) preventing the commission of offences;

d) bringing offenders to justice; and

e) any duty or responsibility of the police arising from common or statue law.

3.16 The code allows the police to disclose police information to other person or bodies where this is reasonable and lawful to do for the policing purposes as set out in 3.15. Any sharing of information must comply with the ACPO Guidance on the Management of Police Information 2006 and any protocol, national or local, which may be agreed with the persons or bodies needing to receive the information.

Appendix 2: Part I - Glossary

In this Protocol the following words shall have the following meaning unless the context otherwise requires:

Ancillary Protocols	Means all and any 'tactical' information sharing protocols entered into pursuant to Clause 2.2;
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;
Crime	Means 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;
Crime and Disorder Information Sharing Protocol	Means the Devon and Cornwall Partnership Information Exchange Protocol entered into by the signatories and others on 1st March 2003.
Data Controller	Means 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	Means any person (other than the 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;
De-personalised Data	Means any information where any reference to or means of identifying a living individual has been removed;
Disclosure	Means a disclosure by one signatory to any other signatory of personal data;
Disorder	Means a level or pattern of anti-social behaviour within a particular area;
DPA 1998	Means the Data Protection Act 1998;
Mental Disorder	Means mental illness, arrested or incomplete development of mind, psychopathic disorder or any other disorder or disability of mind;
Nominated Holder	Means the nominated holder of this Protocol, which shall be the Head of Information Management, Devon & Cornwall Police;
Nominated Officers	Means all those individuals identified in Appendix 3 Part II and any changes to the same notified to the signatories by the nominated holder;
Personal Data	Means data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of or are likely to come into the possession of any signatory. They include, without limitation, any expression of opinion or intentions in respect of such a living individual.
Prevention of Offending	Means activity which reduces the likelihood of offending or re-offending by persons with a mental disorder through the provision of relative information, which will reduce the risk factors associated with offending and promotes protective factors;

Processing	Means obtaining, recording or holding personal data or carrying out any operation or set of operations on the information or data including: (a) organisation, adaption or alteration of the personal data; (b) retrieval, consultation or use of the personal data; (c) disclosure of the personal data by transmission, dissemination or otherwise making available; or (d) alignment, combination, blocking, erasure or destruction of the personal data; and 'Process' shall be interpreted accordingly.
Protocol	Means this protocol;
Purpose	Means the purpose of this Protocol, as set out in Clause 3;
Relevant Authority	Means any of those bodies or persons described in Section 115(2) of the Crime and Disorder Act 1998 and 'Relevant Authorities' shall be interpreted accordingly;
Restricted Information	Means the information contained in this section is not to be considered 'open' information under the Freedom of Information Act. This section of information should not be transmitted over an insecure internet connection.
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;
Signatories	Means the signatories/parties to this Protocol which are identified in clause 1 and, for the avoidance of doubt, "Signatory" shall mean any one of them;
Subject Access Request	Means a request made by a data subject to a signatory pursuant to section 7 of the DPA 1998.

Appendix 2: Part II - Interpretation

1. In this Protocol where the context requires:

    1.1 the masculine gender includes the feminine and the neuter and the singular includes the plural and vice versa;

    1.2 references to any statute or statutory provision include a reference to that statute or statutory provision as from time to time amended, extended or re-enacted and also include any subordinate legislation made thereunder from time to time;

    1.3 references to clauses and appendices are, unless otherwise stated, references to clauses in and Appendices to this Protocol.

2. In this Protocol headings are for ease of reference and shall not affect its interpretation.

3. Subject to paragraph 4 below, the Appendices form part of this Protocol.

4. In the event of any conflict between the provisions contained in this Protocol and the provisions contained in the Appendices, the provision of this Protocol shall prevail and for the purposes of this paragraph 4 only the term ’Protocol‘ shall be deemed not to include the Appendices.

Appendix 3: Restricted Information [FOI Section 40(2) will apply to personal names and tel. numbers in copies published as part of FOI Publication Schemes]

Contact Information - Nominated Officers for Information Requests and Disclosures.

Organisation	Name or Post of Nominated Officer	Name or Post of Backup	Address, Tel. No. & SECURE Email
Devon & Cornwall Police	Detective Inspector Force Intelligence Centre	Detective Sergeant Force Intelligence Centre	Force Headquarters Middlemoor Exeter EX2 7HQ Tel: 01392 452627 **This is a 24 hours number** Fax: 01392 452814 **Secure Email:** FIB@devonandcornwall.pnn.police.uk
Process for accessing information out of hours / in an emergency			
Devon County Council	See Devon Partnership NHS Trust.		See Devon Partnership NHS Trust
Devon Partnership NHS Trust Devon Partnership NHS Trust has operational responsibility for; Devon County Council and Torbay Council	**0830hrs – 1700 hours** Sue Tostevin, Alan Jones or Samantha Taylor Information Governance Administrators Fiona Spencer-Smith IM&T team Administrator Nick Hopkinson Associate Director IM&T Sue Banham or Emmy Lloyd Information Governance Manager Samantha Taylor Alan Jones Fiona Spencer-Smith		Wonford House Hospital, Dryden Road Exeter, Devon EX2 5AF Tel: Tel: 01392 675678 Secure e-mail – ig.dpt@nhs.net Tel: 01392 674128 Or Tel: 01392 208866

Restricted Information **[FOI Section 40(2) will apply to personal names and telephone numbers**			
Organisation	**Name or Post of Nominated Officer**	**Name or Post of Backup**	**Address and Tel No**
Cornwall Council	**During Office Hours:** Sarah McBride, Senior Operations Manager (LD,PD & MH) **Out of hours;** Cornwall Partnership NHS Foundation Trust has out of hours responsibility for Cornwall Council		Old County Hall, Truro Cornwall TR1 3AY Tel: 0300 12341000 Secure e-mail Sarah.mcbride@cornwall.gcsx.gov.uk
Cornwall Partnership NHS FoundationTrust Cornwall Partnership NHS Foundation Trust has out of hours operational responsibility for; Cornwall Council	**Office Hours;** Caldicott Guardian – Ellen Wilkinson. Data Protection Officer - Tim Shaw Associate Director of Compliance – Lorna Watt. **Out of Hours;** On call manager.		Trust Headquarters, Porthpean Rpad, St. Austell PL26 6AD Tel: 01726 291018 01726 291034 Fax: 01726 291207 via Bodmin Hospital Tel: 01208 251300
Council for the Isles of Scilly *NB. The agreement for Mental Health Cover of the Isles of Scilly in still the subject of negotiation	Penelope Penn-Howard Social Services Social Worker Scott Powell J. Roberts **Out of hours** As above		Town Hall St Marys Isles of Scilly TR21 0LW Tel: 01720 422148 Tel: 01872 863562

Restricted Information [FOI Section 40(2) will apply to personal names and telephone numbers			
Organisation	**Name or Post of Nominated Officer**	**Name or Post of Backup**	**Address and Tel No**
NHS Plymouth	**Office Hours** Karen Howard Tracey Ford or Secure group Email address:		Plymouth Teaching Primary Care Trust Mount Gould Hospital Mount Gould, Plymouth PL4 7QD Karen -Tel: 01752 314001 Secure e-mail Ply-pct.plyminfoconstabulary@nhs.net AOS Admin Staff Tel:-1752 314033 Out of hours contact is
Plymouth City Council	Office Hours Contact; Richard Woodfield, Disclosure Officer Out of office hours contact; Richard Lemon, Team Leader		Social & Housing Dept., Floor 1, Winsor House, c/o Civic Centre Plymouth PL1 2AA Tel: 01752 307329 Tel: 01752 346984 Fax: 01752 331193
Torbay Council	See Devon Partnership NHS Trust		See Devon Partnership NHS Trust

Appendix 4: Procedures for Information Requests and Disclosures

1. Making Requests for Disclosures

1.1 All requests for Disclosures should be made by the nominated officer of the relevant signatory and, for the avoidance of doubt, requests made by any other person from the relevant signatory will be declined.

1.2 All requests for disclosures should be sent to the nominated officer of the relevant Signatory.

1.3 All requests for disclosures must be made on the appropriate form, a copy of which is attached at Appendix 5. (The reverse of that form contains references to reasons for disclosures and the appropriate one is to be indicated to support each application for disclosure.)

1.4 Each form submitted in support of a request for disclosure must be delivered by secure email, post or in person. Forms may only be submitted by fax in the event of an emergency, secure email not being available, and after appropriate arrangements have been made for the signatory receiving the request to wait by the receiving fax machine to collect the fax immediately upon delivery.

1.5 Where Statutory Agencies require urgent access to information held by Devon & Cornwall Police, out of normal office hours the process will be:

a) The information request can be made via telephone by a named authorised signature or agreed service area as identified at Appendix 3.

b) Devon & Cornwall Police will verify the caller.

c) The request must be backed up by the submission of a Form MH1 or Potentially Dangerous Person form Appendix 7 or 8, within 72 hours.

2. Making Disclosures in Response to Requests for Disclosures

2.1 All disclosures to a signatory should only be made to the nominated officer of the relevant signatory.

2.2 Disclosures from those signatories with Caldicott Guardians must be endorsed by the relevant Caldicott guardian unless the relevant signatory notifies the nominated holder otherwise.

2.3 All disclosures should be made on the appropriate forms, a copy of which is attached at Appendix 7.

2.4 The signatories should respond to formal requests for disclosure of personal data within forty-eight (48) hours of receipt of the request. However, it is acknowledged that there may be occasions when the disclosure is required more urgently. In such circumstances, response will be made within two (2) hours if it can be demonstrated that:

2.4.1 there is a real threat to the health of a data subject; and / or

2.4.2 it is needed to prevent likely injury to a data subject; and / or

2.4.3 it is needed for the protection of vulnerable members of the community; and / or

2.4.4 it is needed for maintaining public safety; and / or

2.4.5 it is needed for the apprehension of offenders;

and the disclosure may be made prior to a form being submitted pursuant to paragraph 2.3 above. In such instances, and to maintain an adequate disclosure trail, a retrospective request form must be submitted within one (1) working day. In an emergency situation, secure e-mail or faxed confirmation of a request may be made, but for security reasons, no personal data must be disclosed by fax.

2.5 Upon receipt of an application for disclosure, the signatory receiving the application shall first establish whether any of the personal data which is the subject of the application was supplied to it by another signatory. In the event that it was, the signatory receiving the application shall, without delay, contact the signatory from whom the personal data originated who shall, in turn, confirm in writing without delay that:

2.5.1 the personal data remains accurate; and

2.5.2 whether the personal data may be disclosed.

In the event that the personal data originated from the signatory receiving the request for disclosure, that signatory should process the disclosure in accordance with its normal procedures.

3. Disclosures at Meetings

3.1 Signatories who anticipate making disclosures at meetings should ensure they are empowered to do so and that such disclosures are permitted by all relevant legislation prior to making any disclosure.

3.2 Such disclosures should be recorded within the minutes of the relevant meeting and the relevant signatory or signatories shall ensure that these minutes are retained for at least six (6) years.

3.3 It is suggested as a model of good practice, that those signatories making disclosures at meetings should clarify all issues reasonably relevant to any intended disclosure, to include without limitation confidentiality issues and powers to make the disclosure, prior to the commencement of the relevant meeting.

4. General

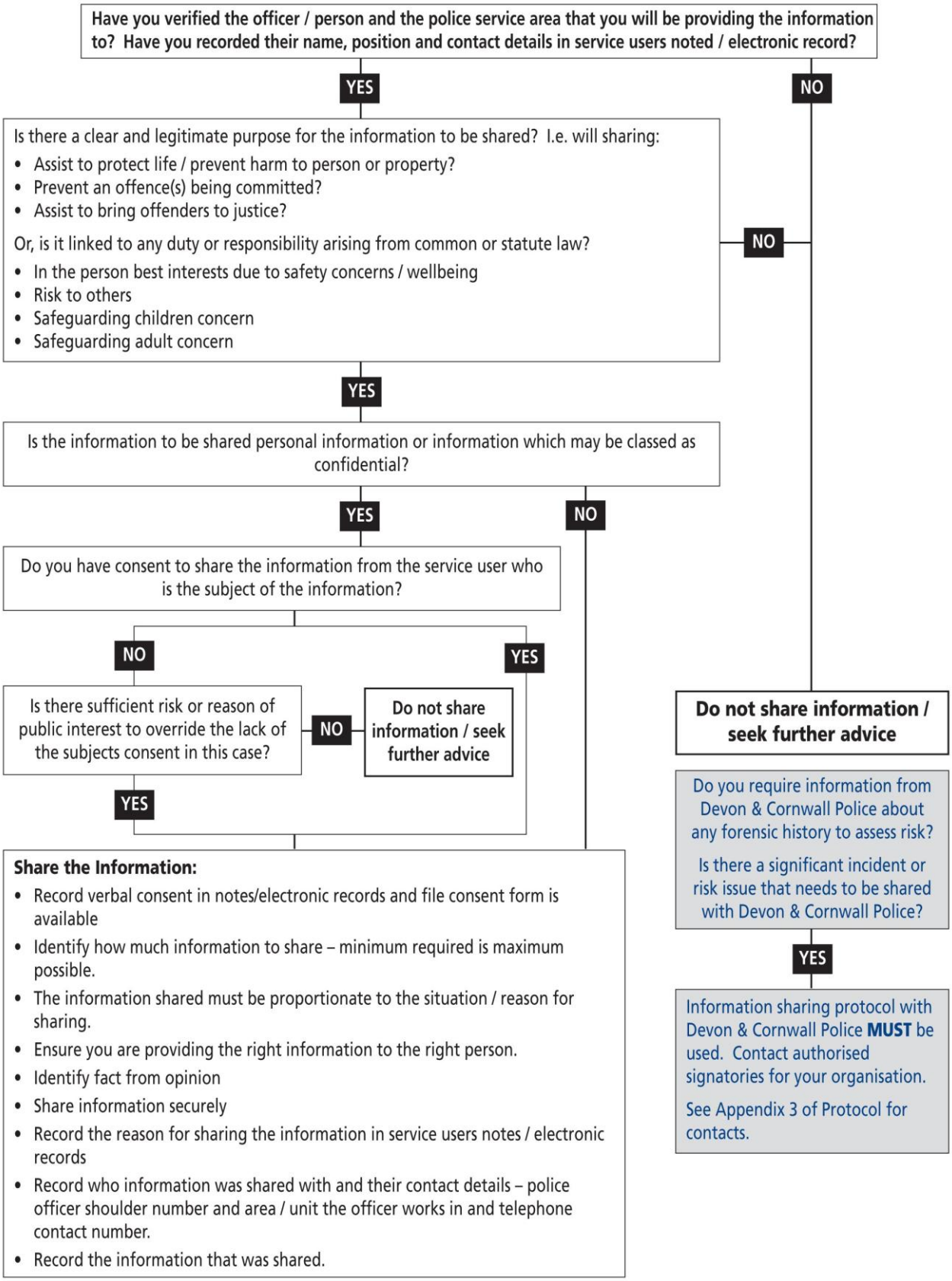
4.1 All queries regarding any disclosures to be or being made or which have been made by a signatory shall only be addressed to the nominated officer of that signatory.

4.2 All queries relating to the strategic use of the Protocol shall be referred to the relevant nominated officer identified in Appendix 3 Part I.

Appendix 5

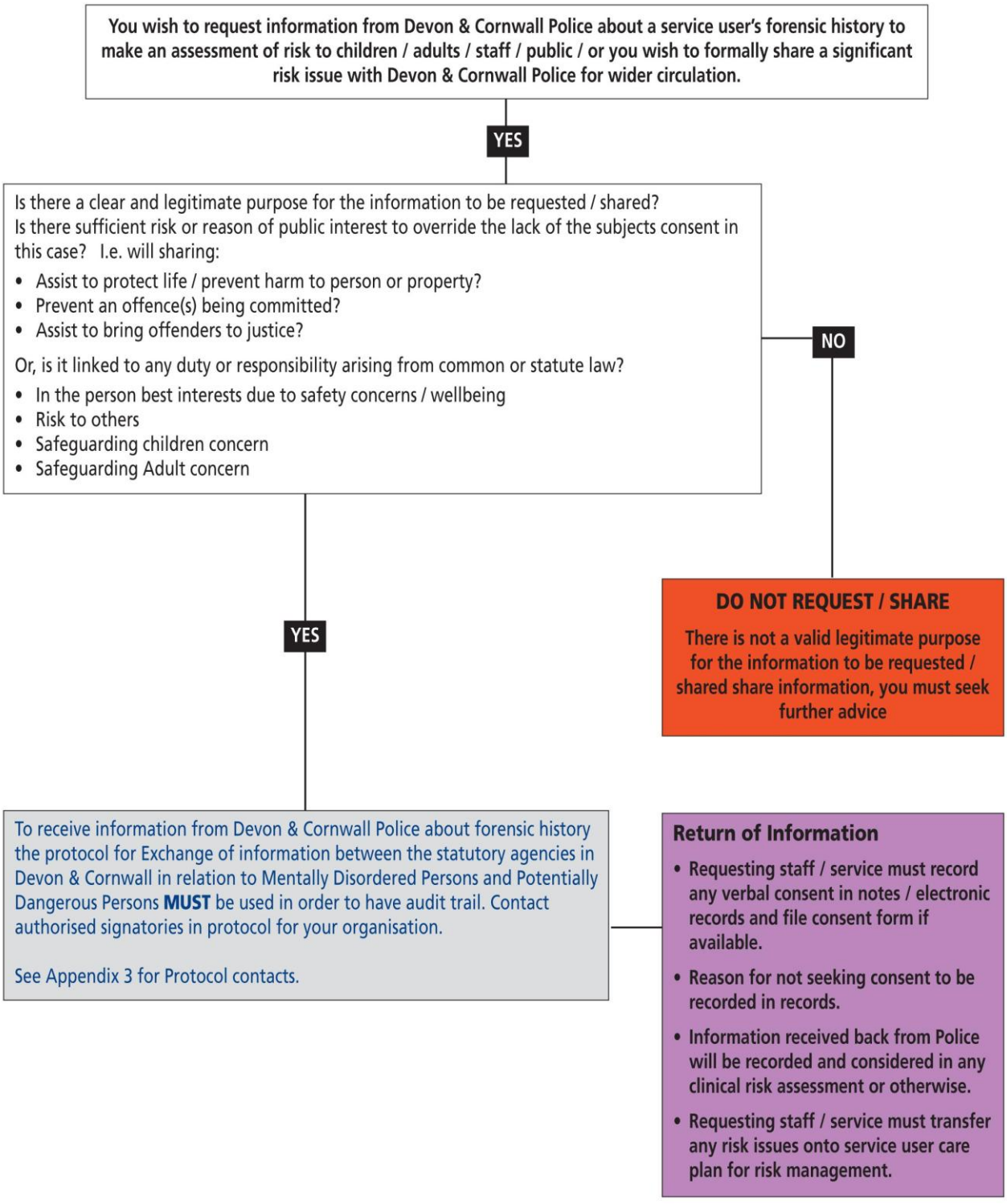
Information Sharing Flow Chart for Health / Social Care Staff - February 2010

Devon & Cornwall Police request information about service users / or who wish to share information with Devon & Cornwall Police about a service user



Appendix 6

Information Sharing Flow Chart for Health / Social Care Staff - February 2010



Appendix 7: Form MH1

*Request / Disclosure of Personal Information (Mental Health) (*Circle as appropriate)

Police Ref. (Prefix of DCP/request no./year) (Use new request. This is the unique master/ref. no.)		Trust / Council Ref. (PMH/request no./year) Use new request. This is the unique master/ref. no.)
DCP:		PMH:
Update of previous information? ☐ Yes ☐ No Master unique reference (use this for updating information)		
DCP:		PMH:
Priority: ☐ Within 2 hours ☐ Routine within 48 hours (tick as appropriate)		
Person's Details		
Last name/family name:		First name(s):
Alias:	Date of Birth:	Place of Birth:
Address:		Postcode:
Ethnicity (tick boxes): 1. White ☐ 2. Mixed ☐ 3. Asian or Asian British ☐ 4. Black or Black British ☐ Chinese or other ethnic group ☐		
Distinguish marks / unique features:		
Reason for request / disclosure for information: ☐ Risk / ☐ Harm (*Circle as appropriate)		
Consent: *Sought/Obtained *Sought/Refused *Consent not Sought (*Circle as appropriate)		
Reasons for not seeking consent:		
Information required: 1. Previous convictions / Warning and Cautions ☐ 2. Circumstances of arrest ☐ 3. Weapons ☐ Violence ☐ Drug / alcohol use/risks ☐ Risk to children ☐ Risk to vulnerable adults ☐		
☐ Risk of inappropriate sexual behaviour ☐ Risk to staff ☐ Any other risks (please not below)		
Requested by (print name and designation of authorized signatory):		
Date:		
Contact person and Tel. No. (include code):		

Health / Social Services to use this form when disclosing information about significant events / risks to Devon & Cornwall Police

Trust / Council Ref. No. (as recorded at top of page 1): PMH:				
Person's Details				
Last name/family name:		First name(s):		
Alias:	Date of Birth:		Place of Birth:	
Category of Risk				
Please tick relevant box	High Risk	Medium Risk	Low Risk	Comments / Effects on Risk
☐ Harm to self	☐	☐	☐	
☐ Violence towards others	☐	☐	☐	
☐ Violence towards property	☐	☐	☐	
☐ Weapons	☐	☐	☐	
☐ Abuse of illicit drugs / alcohol / prescription medication (delete as required)	☐	☐	☐	
☐ Failure to take medication	☐	☐	☐	
☐ Absconding	☐	☐	☐	
☐ No fixed abode	☐	☐	☐	
☐ Risk to children	☐	☐	☐	
☐ Fear of uniforms	☐	☐	☐	
☐ Adverse reaction / fear of authority	☐	☐	☐	
☐ Other (please state)	☐	☐	☐	
Other comments to include: ☐ Mental health problems ☐ Learning disability ☐ Epilepsy				
Current risk / trigger factors:				
Name and designation:				
Signature and date:				

Heath / Social Services to use this form when disclosing information about significant events / risks to Devon & Cornwall Police

Trust / Council Ref. No. (as recorded at top of page 1): PMH:		
Person's Details		
Last name/family name:	First name(s):	
Alias:	Date of Birth:	Place of Birth:
Continuation Sheet		
Name and designation:		
Signature and date:		

Appendix 8: Proactive Disclosure under Potentially Dangerous Persons Protocol

Definition of Potentially Dangerous Person

A person who has not been convicted of, or cautioned for, any offence placing them in one of the three MAPPA categories, but whose behaviour gives reasonable grounds that there is a present likelihood of them committing an offence or offences that will cause serious harm.

Definition of Serious Harm

As defined in Section 224(3) of the Criminal Justice Act as 'death or serious personal injury whether physical or psychological'.

Information provider	
☐ Devon & Cornwall Police	☐ Cornwall Council
☐ Cornwall Partnership NHS Foundation Trust	☐ Devon County Council
☐ Devon Partnership NHS Trust	☐ The Council for the Isles of Scilly
☐ Plymouth City Council	☐ Plymouth Primary Care Trust
☐ Torbay Council	☐ Voluntary sector; partner (cite):
Person presenting risk	
Name:	Date of Birth:
Address:	
Ethnicity:	
Nature of risk posed	
Nature and pattern of the person presenting risky behaviour:	
Nature of risk:	
Who is at risk (e.g. particular individuals, children, vulnerable adults):	
In what circumstances is likely to increase (e.g. issues relating to mental health, medication, drugs, alcohol, housing, employment, relationships):	
What factors are likely to reduce risk?	
In your professional judgement do any of the above factors indicate that there is a present liklihood of the individual causing serious harm?	

Power cited as basis of disclosure (tick any that are valid)			
☐	**Crime & Disorder Act 1998 – Section 115:** Disclosure of information to a relevant authority to prevent or detect crime and disorder.		
☐	**Data Protection Act 1998 – Section 29(3):** Disclosure for the prevention or detection of crime, apprehension and prosecution of offenders.		
☐	**MoPI Police Act 1996 (Police Only) – Policing Purpose:** Protecting life and property, and preventing the commission of offences. – N.B. Cannot be used in isolation, does require to be supported by statute or common law		
☐	**Common Law:** Will disclosure aid prevention / detection of crime?		
Tests applied to provision of information			
Justification under Human Rights: Is the disclosure:			
(a)	in accordance with the law?	☐ Yes	☐ No
(b)	in the interests of public safety?	☐ Yes	☐ No
(c)	for the protection of health and morals? (e.g. where the person is involved in drug dealing or procuring for prostitution etc.)	☐ Yes	☐ No
(d)	for the protection of rights and freedoms of others?	☐ Yes	☐ No
(e)	is the circumstances proportional? (if yes – give details below)	☐ Yes	☐ No
(f)	has the information provider's records been updated to record the proposed disclosure?	☐ Yes	☐ No
Identify and list names / contact details of other agencies who are / need to be involved with the person presenting risk or informed.			
Information to be verified and endorsed by SPOC for referring agency:			
Signed (SPOC):		Date:	

Submit to D&C Police HQ PPU via fax: 01392 452814 or via secure email to FIB@devonandcornwall.pnn.police.uk

Appendix 9:

1. Subject access requests and other rights of data subjects

1.1 The signatories acknowledge that data subjects have, amongst other rights, a right to access certain personal data relating to them held by or under the control of data controllers pursuant to Section 7 of the DPA 1998.

1.2 The signatories agree that they shall apply their own internal procedures to dealing with subject access requests made in respect of access to personal data held by them. Where the subject access request relates in whole or in part to personal data received from other signatories through a disclosure the signatory in receipt of the subject access request shall also apply the Subject Access Request Procedure set out in Appendix 7.

1.3 The signatories shall each comply with their own internal procedures when dealing with notices received from data subjects which are made under the Data Protection Act 1998 in respect of personal data held by them. Where the notice relates in whole or in part to personal data received from other signatories through a disclosure the signatory in receipt of the notice shall, where reasonably appropriate, consult with the signatories who made the disclosures.

1.4 The signatories shall each comply with the provisions of the DPA 1998 when handling subject access requests and any other notices received from data subjects which are made under the Data Protection Act 1998.

1.5 The signatories recognise that the Data Protection Act 1998 does not cover data relating to deceased persons and that, accordingly, requests received from third parties for access to data relating to deceased persons will not be treated in the same manner as subject access requests. The signatories recognise that access to such data is covered by the Access to Health Records Act 1990 (as amended) and the common law of confidentiality. The signatories agree that request for access to such data will be dealt with in accordance with their own respective internal procedures with consultation with other signatories where reasonably appropriate in the event that any of the data concerned originated from such other signatories by means of a disclosure.

2. Procedures for handling subject access requests

2.1. All signatories should have internal procedures in place for handling and responding to subject access requests (i.e. requests for access to personal data made pursuant to Section 7 of the Data Protection Act 1998).

2.2. The following procedures should also be used for dealing with subject access requests in respect of personal data which is held for crime and disorder purposes:

2.3 On receipt of a subject access request, if the request refers only to personal data processed by the signatory receiving the request, that signatory should follow its own standard procedures for dealing with such requests.

2.4. On receipt of a subject access request, if the request refers to any personal data which originated from another signatory it will be the responsibility of the signatory receiving the subject access request to contact the signatory from whom the personal data originated via the nominated contact person to determine whether they wish to claim an exemption to withhold the personal data under the provisions of the Data Protection Act.

2.5 Any decisions made to withhold personal data from a data subject should be taken with care, and if necessary, legal or other appropriate professional advice sought. They should also be formally recorded in case of subsequent dispute. There is no requirement to inform the data subject requesting access that personal data has been withheld from them for these purposes.

3. Third party information

3.1 When a signatory cannot comply with a subject access request without disclosing information relating to another **individual** who can be identified from that information the provisions of Sections 7 and 8 of the Data Protection Act 1998 shall govern whether or not the disclosure is made to data subject making the subject access request.

4. Time limit for dealing with subject access requests

4.1 Subject access requests must be dealt with as quickly as possible in order to ensure that the signatories are able to respond to the subject access request within the 40 day period required by statute from the date that sufficient information is received from the data subject that enables the signatory to process the subject access request.

Appendix 10: Matrix for Coding of Information Requests within the Protocol

Set out below is the code to be used on the relative requests for information under this protocol. The code numbering system will assist the audit process for requests and disclosures and prevent the duplication on information related to ongoing incidents. Can you please ensure that this code structure is introduced on requests with immediate effect.

Partner Organisation	Code for Requests	Code for Requests example
Devon & Cornwall Police	D&CC/No/Year	D&CC/05/2004
Cornwall Council	CC/No/Year	CCC/05/2004
Cornwall Partnership NHS FoundationTrust	CPT/No/Year	CPT/05/2004
Devon County Council	DCC/No/Year	DCC/05/2004
Devon Partnership NHS Trust	DPT/No/Year	DPT/05/2004
The Council for the Isles of Scilly	CIS/No/Year	CIS/05/2004
Plymouth City Council	PCC/No/Year	PCC/05/2004
Plymouth Primary Care Trust	PPC/No/Year	PPC/05/2004
Torbay Council	TC/No/Year	TC/05/2004