

# Crime and Disorder Act 1998

## Devon and Cornwall Partnership Information Exchange Protocol For Crime and Disorder



V2.0 POST ACPO DP MOG, MOPI, AND POLICE AND JUSTICE ACT 2006

NOVEMBER 2007.

## CONTENTS

1. Parties/Signatories
2. Purpose
3. Definitions and Interpretation
4. Core Objectives and Standards
5. Law Governing and Enabling the Exchange of Personal Data Under this Protocol
6. Scope and Requests for the Disclosure of De-personalised Information
7. Legality of Disclosures
8. Procedures for Disclosing Data
9. Nominated Officers
10. Registration/Notification under the DPA 1998
11. Compliance with the DPA 1998
12. Accuracy of Data
13. Data Standards
14. Use of Personal Data and Confidentiality
15. Security
16. Agents, Contractors and Service Partners
17. Retention and Disposal of Personal Data
18. Subject Access Requests and other Rights of Data Subjects
19. Complaints
20. Compliance and Good Practice
21. Regular Review of Protocol and Consultation Regarding Protocol
22. Changes to the Protocol
23. Changes to Signatories
24. Indemnity
25. Publication of Protocol
26. Race Relations (Amendment) Act 2000 Impact Statement
27. Third Party Rights
28. Counterparts
29. Certification
30. Revision Information

- APPENDIX ONE: Part I: Glossary  
Part II: Interpretation
- APPENDIX TWO: Contact Information
- APPENDIX THREE: Procedures for Information Requests and Disclosures
- APPENDIX FOUR: Request for Disclosure of Personal Data Form
- APPENDIX FIVE: Disclosure of Personal Data Form
- APPENDIX SIX: Restrictions on the Disclosure of Personal Data
- APPENDIX SEVEN: Procedures for Handling Subject Access Requests
- APPENDIX EIGHT: Disclosable Data

**CRIME AND DISORDER ACT 1998**  
**DEVON AND CORNWALL PARTNERSHIP**  
**INFORMATION EXCHANGE**  
**PROTOCOL FOR CRIME AND DISORDER**

---

***1. PARTIES/SIGNATORIES***

1.1 The Signatories to this Protocol are:

- 1.1.1 Devon and Cornwall Constabulary
- 1.1.2 Devon and Cornwall Police Authority
- 1.1.3 Cornwall & Isles of Scilly Primary Care Trust
- 1.1.4 Cornwall Council
- 1.1.5 Cornwall Partnership NHS Trust
- 1.1.6 Council of the Isles of Scilly
- 1.1.7 Devon County Council
- 1.1.8 Devon & Somerset Fire & Rescue Service
- 1.1.9 Devon Partnership NHS Trust
- 1.1.10 Devon Primary Care Trust
- 1.1.11 East Devon District Council
- 1.1.12 Exeter City Council
- 1.1.13 Mid-Devon District Council
- 1.1.14 National Probation Service, Devon and Cornwall Probation Area
- 1.1.15 North Devon District Council
- 1.1.16 Northern Devon Healthcare NHS Trust
- 1.1.17 Plymouth Hospitals NHS Trust
- 1.1.18 Plymouth City Council
- 1.1.19 Plymouth Primary Care Trust
- 1.1.20 Royal Cornwall Hospitals NHS Trust
- 1.1.21 Royal Devon and Exeter NHS Foundation Trust
- 1.1.22 South Devon Healthcare NHS Foundation Trust
- 1.1.23 South Hams District Council
- 1.1.24 South West Peninsula Health Authority
- 1.1.25 South Western Ambulance Service NHS Trust
- 1.1.26 Teignbridge District Council
- 1.1.27 Torbay Council
- 1.1.28 Torbay Care Trust
- 1.1.29 Torridge District Council
- 1.1.30 West Devon Borough 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 Two.

## **2. Purpose**

- 2.1 The purpose of this Protocol is to facilitate the exchange of information (including Personal Data) between the Signatories in furtherance of the compliance of relevant Signatories 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.
- 2.2 This Protocol shall provide the framework for the exchange of information described in clause 2.1. The Signatories agree that further information sharing protocols and working practice agreements ancillary to this Protocol, shall, where appropriate, be entered into by the Signatories to cover such information exchange in relation to specific areas of work.

## **3 Definitions and Interpretation**

- 3.1 All defined terms used throughout this Protocol are described in the Glossary contained at Part I of Appendix One to this Protocol.
- 3.2 This Protocol shall be interpreted in accordance with all and any rules of interpretation set out in Part II of Appendix One.

## **4 Core Objectives and Standards**

- 4.1 The Signatories when preparing this Protocol subscribe to the core objectives and standards set out in clause 4.3 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.
- 4.2 The Signatories agree that all Ancillary Protocols shall comply with the core objectives and standards set out in clause 4.3.
- 4.3 The core objectives and standards referred to in clauses 4.1 and 4.2 are:
- 4.3.1 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;
- 4.3.2 the protocol must set out the legal basis for the exchange of the information covered by the protocol;
- 4.3.3 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;
- 4.3.4 the common law principles of confidentiality should be upheld;
- 4.3.5 the rights of the Data Subjects and other individuals under The Human Right Act 1998 should be upheld;
- 4.3.6 the protocol should be reviewed on a regular basis and in the light of new legislation and/or official guidance; and
- 4.3.7 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.

## **5 Law Governing and Enabling the Exchange of Personal Data Under this Protocol**

### Legal Power to Make Disclosures

- 5.1 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 [see 5.2.6. below].

### Data Protection Act 1998

- 5.2 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:
- 5.2.1 section 29 (for the prevention or detection of crime, the apprehension or prosecution of offenders, and taxation purposes);
  - 5.2.2 section 34 (where information is to be made available to the public by or under enactment);
  - 5.2.3 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);
  - 5.2.4 section 28 (for the purpose of safeguarding national security);
  - 5.2.5 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.

- 5.2.6. The Data Protection Act 1998 Schedule 2 & 3 Condition that **may** apply in the exchange of information within this protocol are as follows;

**Schedule 2:** Conditions Relevant for the First Principle; Processing of **Personal Data**; One or more condition required.

- 1 With the consent of the data subject.
- 3. The processing is necessary for the compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- 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
  - (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 third party or parties to whom the data are disclosed, except where processing is unwarranted in any particular case by reason of prejudice to rights and freedoms or legitimate interests of the data subject.

**Schedule 3: Conditions Relevant for the First Principle; Processing of Sensitive Personal Data; One or more condition required.**

- 1 With the explicit consent of the data subject.
- 2 The processing is necessary-
  - (a) in order to protect the vital interests of the data subject or another person, in a case where;
    - (i) consent cannot be given by or on behalf of the data subject, or
    - (ii) the data controller cannot be reasonably be expected to obtain the consent of the data subject, or
  - (b) in order to protect the vital interest of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
- 6 The processing-
  - (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
  - (b) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.),
- 7 (1) The processing is necessary-
  - (a) for the administration of justice,
  - (b) for the exercise of any function conferred on any person by or under an enactment.

Crime and Disorder Act 1998 section 115

- 5.3 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.
- 5.4 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.
- 5.5 Where a Relevant Authority are using contacted organisations from the private or voluntary sector to assist in the delivery of services **and** this contracted agency receive information provided under this protocol, these agencies will not be deemed as full signatory partners to the Protocol. However, any necessary and relevant information disclosures can be made to these contacted organisations under Section 115 (1) (a) of the Crime and Disorder Act 1998 in that the contracted organisation will be deemed to 'a person acting on behalf of such a (relevant) authority'. The Relevant Authority will be expected to have a robust data disclosure agreement in place as part of its contract with the organisation, as per Section 16 below..

The Code of Practice on the Management of Police Information.

- 5.6. This code was developed under section 39 and 39a of the Police Act 1996 and enacted in November 2005. 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.

- 5.7. 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 statute law.
- 5.8. 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 5.7. 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.
- 5.9. Additionally the Code of Practice sets out obligations on the persons or bodies receiving police information which equate to the requirements set out in section 5.2, 5.11, 8.3, 11.1, 12, 14,15 and 17 of this protocol

#### Consent

- 5.10. 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. Note that Data Subject consent is also subject to the Caldicott Principles outlined in Section 8.2. and Appendix 3.

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

- 5.11. 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:
- 5.11.1 The Data Protection Act 1998;
  - 5.11.2 The Human Rights Act 1998; and
  - 5.11.3 the common law duty of confidence.
- 5.12. The Signatories should confirm, check and verify compliance with the requirements of the legal obligations on each of them described in clause 5.11.
- 5.13. 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.
- 5.14. For the purposes of clause 5.13, the Signatories understand the public interest criteria to include (but not be limited to):
- 5.14.1. the administration of justice;
  - 5.14.2. maintaining public safety;
  - 5.14.3. the apprehension of offenders;
  - 5.14.4. the prevention of Crime and Disorder;
  - 5.14.5. the detection of Crime; and
  - 5.14.6. the protection of vulnerable members of the community.
- 5.15. The Signatories should confirm, check and verify the following points when deciding if the public interest criteria should override any duty of confidentiality:

- 5.15.1. That the intended Disclosure proportionate to the intended aim
- 5.15.2. The vulnerability of those who are at risk where this is a factor to support disclosure
- 5.15.3. The likely impact of the Disclosure on the Offender
- 5.15.4. That there is no other equally effective means of achieving the same aim
- 5.15.5. That the Disclosure necessary to prevent or detect Crime and uphold the rights and freedoms of the public?
- 5.16. The necessary to disclose the information, to protect other vulnerable people?
- 5.17. The Signatories should confirm, check and verify 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:
  - 5.17.1. national security;
  - 5.17.2. public safety;
  - 5.17.3. economic well being of the country;
  - 5.17.4. the prevention of crime and disorder;
  - 5.17.5. the protection of health and morals; or
  - 5.17.6. the protection of the rights or freedoms of others

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

- 5.18. The Signatories should confirm, check and verify 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 5 from time to time Provided 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.

## **6 Scope and Requests for the Disclosure of De-personalised Information**

- 6.1 This Protocol is primarily concerned with the exchange of Personal Data between the Signatories.
- 6.2 The Signatories agree that Disclosures of Personal Data shall not be made under this Protocol where a disclosure of De-personalised Data would, instead, suffice. For example, De-personalised Data consisting of aggregated data or statistical data may instead be disclosed.
- 6.3 In the event the disclosure of De-personalised Data, including disclosures made under the Crime & Disorder (Prescribed Information) Regulations 2007, the Signatory receiving the request shall make the disclosure requested subject to the following conditions:
  - 6.3.1 the De-personalised Data shall only be used for the purpose for which it is requested and that that purpose shall accord with the Purpose;
  - 6.3.2 the De-personalised Data shall not be Processed in such a way that information about a living individual may be extracted from the De-personalised Data.

## **7. Legality of Disclosures**

- 7.1 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.

- 7.2 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.
- 7.3 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.

## **8. Procedures for Disclosing Data**

### Procedures in Appendix Three

- 8.1 The Signatories shall follow the procedures set out in Appendix Three when requesting and making Disclosures and shall be mindful of the restrictions on Disclosures detailed in Appendix Six.

### Caldicott

- 8.2 The Signatories also acknowledge that those Signatories in the health sector or which have Social Services Departments 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 must comply with these. Those Signatories in the health sector or which have Social Services Departments shall notify the Nominated Holder of all and any such procedures with which they expect Signatories requesting a Disclosure to comply with and the Nominated Holder shall circulate details of the same to the Signatories.

Direct information exchange between a Hospital NHS Trusts and the Devon & Cornwall Constabulary will utilize the Information Sharing Protocol agreed between the Constabulary and Bevan Ashford in 2002, where the specific information request is linked to the three areas of this protocol and the Hospital is a signatory to this protocol

### Compliance with law, this Protocol and internal policies

- 8.3 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.

### Minimum Disclosure Necessary

- 8.4. 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.

### Proportionality

- 8.5 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.

### Disclosable Personal Data

- 8.6 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 Eight.

## **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 Two.
- 9.2 The relevant Nominated Officer 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.

## **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 11.1, 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 One 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 which 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 endeavour 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 Confidentiality**

##### Process in accordance with Purpose

- 14.1 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 Three.

##### Confidentiality

- 14.2 Each Signatory shall at all times keep confidential all Personal Data supplied pursuant to this Protocol.

##### Publication of Personal Data

- 14.3 Signatories may only publish Personal Data disclosed to them by another Signatory pursuant to this Protocol if such Personal Data is anonymised and presented in such a way that it is De-personalised Data.

##### Disclosure of Personal Data to Another Signatory

- 14.4 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.

- 14.5 This clause 14 shall survive termination of the Protocol or the withdrawal of or removal of any Signatory.

#### **15. Security**

- 15.1 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.

- 15.2 The Devon and Cornwall Constabulary will grade the Personal Data provided to them, to restrict access, where this is applicable.

- 15.3 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.

- 15.4 The Signatories recognise the merit of maintaining a full audit record of all Disclosures made to them.

- 15.5 The Signatories acknowledge that the national standard for making data (including Personal Data) secure is industry standard BS7799. 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.

15.6 The provisions of this clause 15 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;

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. Retention and Disposal of Personal Data**

17.1 The Signatories acknowledge that Schedule One of the DPA 1998 provides that excessive Personal Data must not be retained.

17.2 The Signatories agree that they must destroy Personal Data provided to them under this Protocol as soon as it is no longer required for the original purpose for which it was supplied or collected.

17.3 In order to meet their obligations under clause 17.1, all Signatories are expected to introduce a procedure and nominate a person to conduct reviews of Personal Data received through a Disclosure on a regular basis and at least every six (6) months.

**18. Subject Access Requests and Other Rights of Data Subjects**

18.1 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.

18.2 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 Seven.

- 18.3 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.
- 18.4 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.
- 18.5 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.

## **19 Complaints**

- 19.1 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.
- 19.2 Signatories will keep each other informed of developments following a complaint received, where relevant.

## **20. Compliance and Good Practice**

- 20.1 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. Regular Review of Protocol and Consultation Regarding Protocol**

- 21.1 The Nominated Holder shall ensure that a review of the Protocol is carried out by the Signatories:
- 21.1.1. within the first six (6) months of the date of the Protocol being signed;
  - 21.1.2 on an annual basis; and
  - 21.1.3 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.
- 21.2 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 the Protocol**

- 22.1 All and any signatories may request any change to the Protocol at any time by submitting a request to the Nominated Holder.
- 22.2 Upon receipt of any requests for changes to the Protocol the Nominated Holder shall:
- 22.2.1 circulate the requests to all the Signatories;
  - 22.2.2 co-ordinate responses received from any Signatories to the same; and
  - 22.2.3 where appropriate, seek the agreement to the requested changes from the Signatories.
- 22.3 No change shall be made to the Protocol except with the agreement of all of the Signatories, which agreement shall be recorded in writing.
- 22.4 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.

## **23. Changes to Signatories**

### Withdrawal/Removal of Signatory from Protocol

- 23.1 Any Signatory may withdraw from being a Signatory to this Protocol upon giving written notice to the other Signatories.
- 23.2 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.
- 23.3 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].
- 23.4 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.
- 23.5 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.

### Additional Signatories

- 23.6 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 or section 115 of the Crime and Disorder Act 1998.
- 23.7 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.

## **24. Indemnity**

24.1 In consideration of the agreement to make disclosures of Personal Data in accordance with this Protocol, each Signatory shall indemnify all other Signatories and keep them fully and effectively indemnified against all direct losses, claims, damages, liabilities (whether criminal or civil), costs, charges, expenses (including legal fees and costs), demands, proceedings and actions which all, or any, of the other Signatories may incur or which may be established against them by any person and which in any case arises out of:

- any breach by the Indemnifying Signatory, its servants or agent, of any of the provisions of the protocol.
- any processing by the Indemnifying Signatory, its servants or agents, of Personal Data received, for purposes other than the originating purpose, or
- any breach of 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.

Each Signatory shall be under a duty to mitigate against all losses, which it may incur.

## **25. Freedom of information Act 2000 - Publication of Protocol**

25.1 This Protocol is accepted as a document for disclosure in line with the public authority partner's duties under the Freedom of Information Act 2000, and can be included in its Publication Scheme.

## **26 Race Relations (Amendment) Act 2000 Impact Statement**

26.1 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.

## **27 Third Party Rights**

27.1 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.

## **28 Counterparts**

28.1 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.

**29. Certification** – DEVON AND CORNWALL PARTNERSHIP INFORMATION EXCHANGE PROTOCOL FOR CRIME AND DISORDER

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

Signed .....(Insert signature)

..... (Enter name and position of person signing)

for and on behalf of

Date (Insert date)

**30. Revision Information**

| Version No          | Date of Version          | Nature of Amendment  |
|---------------------|--------------------------|--|
| Revised Version 1.0 | January 2003             | Complete revision of document by agreed working party in line with HO recommendations and in consultation with all partners  |
| Revised Version 1.1 | January 2003             | Updates of Contact Names; Corrections within Appendix 8  |
| Revised Version 1.2 | March 2003               | Circulation of amended protocol with certified list of partners<br><i>Update of Police Contacts re Launceston IIMU</i>   |
| Revised Version 1.3 | September 2003           | Plymouth Hospitals NHS Trust details added 4/4/03<br>Contact point for Plymouth City Council added 23/4/03<br>Devon Partnership NHS Trust added 22/5/03<br>Torquay Council contact officer corrected 27/5/03<br>Teignbridge DC contact points amended 08/09/03 |
| Revised Version 1.4 | September 2004           | North & East Cornwall PCT, North Devon PCT Teignbridge PCT and Torbay PCT added to the signature list<br>Royal Devon & Exeter NHS Foundation Trust added in place of RD&E Healthcare Trust   |
| Revised Version 1.4 | November 2004/March 2005 | North Devon PCT Appendix 8 added.<br>Westcountry Ambulance Service Trust NHS Trust added to signature list and full contact list added   |

| Version No  | Date of Version | Nature of Amendment   |
|-------------|-----------------|---|
| Version 2.0 | November 2007   | <p>Section 1.1 &amp; Appendix 2, Part 1 &amp; 2, addition of Devon &amp; Somerset Fire and Rescue Service as per Schedule 6 of Police and Justice Act 2006</p> <p>Addition of Section 5.2.6. to include Data Protection Act Schedule 2 &amp; 3 Conditions.</p> <p>Addition of new section 5.5. Use of contracted organisations as agents of relevant authorities. Subsequent clauses in this section renumbered.</p> <p>Section 5.6 to 5.9.: New section to include direction on information sharing provided within the Code of Practice on the Management of Police Information, and the underpinning ACPO Manual of Guidance.</p> <p>Section 5.10.: Amended to reflect that the Data Subject's consent is subject to the Caldicott principles.</p> <p>Section 6.3: Amended to include reference to the Crime and Disorder (Prescribed Information) Regulations 2007, which came into effect 1<sup>st</sup> August 2007.</p> <p>Sections 5.15 - 5.18 and 8.2: Amended to enforce expectations re compliance with relevant legislation.</p> <p>Section 24: Replacement of previous Indemnity Clause with new version extracted from DCC documents.</p> <p>Section 25: Change of designation to 'Open' document under the FoIA.</p> <p>Appendix 2 Change of points of contact for Carrick DC &amp; Cornwall CC and change of Police Designated Officer role in Caradon &amp; N.Cornwall</p> <p>Change of name to Torbay Care Trust from Torbay Primary Care Trust.</p> <p>Appendix 1: definition of "Working practice agreements ancillary to this Protocol" added</p> <p>Appendix 3 Section 1.3 amended re requests for information in statement format and subsequent use in court hearings</p> |
| Version 2.1 |                 | <p>Section 1.2 – Cornwall CC changed to Cornwall Council &amp; all Cornwall DC removed</p> <p>Appendix 2 Part 2: July 09 – all Cornwall DC removed + Change of Contact points for RD&amp;E NHS Foundation Trust &amp; Northern Devon</p>  |

|  |  |   |
|--|--|---|
|  |  | Healthcare Trust<br>Section 1 & Appendix 2 : Name change to South Devon Healthcare NHS Foundation Trust<br>Appendix 2-part 1 & 2: Contact points for Mid Devon District Council updated Feb 2011. |
|--|--|---|

## APPENDIX ONE

### PART I: GLOSSARY

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

|                                |  |
|--------------------------------|--|
| <b>“Ancillary Protocols”</b>   | means all and any information protocols entered into pursuant to clause 2.2;   |
| <b>“Anti-social Behaviour”</b> | 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;                |
| <b>“Crime”</b>                 | 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; |
| <b>“Data Controller”</b>       | 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;         |
| <b>“Data Processor”</b>        | means any person (other than the employee of the data controller) who processes the data on behalf of the data controller;   |
| <b>“Data Subject”</b>          | means an individual who is the subject of Personal Data;   |
| <b>“De-personalised Data”</b>  | means any information where any reference to or means of identifying a living individual has been removed;   |
| <b>“Disclosure”</b>            | means a disclosure by one Signatory to any other Signatory of Personal Data;   |
| <b>“Disorder”</b>              | means a level or pattern of Anti-social Behaviour within a particular area;  |
| <b>“DPA 1998”</b>              | means the Data Protection Act 1998;  |
| <b>“Nominated Holder”</b>      | means the nominated holder of this Protocol, which shall be the Head of Information Management of Devon and Cornwall Constabulary;   |
| <b>“Nominated Officers”</b>    | means all those individuals identified in Appendix Two Part II and any changes to the same notified to the Signatories by the Nominated Holder in accordance with clause 9.3;                |

|   |  |
|---|--|
| <b>“Personal Data”</b>  | means data which relates to a living individual who can be identified from those data, or from those data and other information which are 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.   |
| <b>“Processing”</b>   | means obtaining, recording or holding Personal Data or carrying out any operation or set of operations on the information or data including: <ul style="list-style-type: none"> <li>(a) organisation, adaptation or alteration of the Personal Data;</li> <li>(b) retrieval, consultation or use of the Personal Data;</li> <li>(c) disclosure of the Personal Data by transmission, dissemination or otherwise making available; or</li> <li>(d) alignment, combination, blocking, erasure or destruction of the Personal Data;</li> </ul> <p>and “Process” shall be interpreted accordingly.</p>   |
| <b>“Protocol”</b>   | means this protocol;   |
| <b>“Purpose”</b>  | means the purpose of this Protocol, as set out in clause 2;  |
| <b>“Relevant Authority”</b>                                     | 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;   |
| <b>“Sensitive Personal Data”</b>                                | means Personal Data consisting of information as to- <ul style="list-style-type: none"> <li>(a) the racial or ethnic origin of the Data Subject,</li> <li>(b) his political opinions,</li> <li>(c) his religious beliefs or other beliefs of a similar nature,</li> <li>(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),</li> <li>(e) his physical or mental health or condition,</li> <li>(f) his sexual life,</li> <li>(g) the commission or alleged commission by him of any offence, or</li> <li>(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;</li> </ul> |
| <b>“Signatories”</b>  | 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;   |
| <b>“Working practice agreements ancillary to this Protocol”</b> | means specialised working practices agreed with specific partners which use the C&DA 1998 as the main power for disclosure, and directly link to the aims of this protocol e.g. disclosure of police images to council CCTV units.   |

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

## **APPENDIX THREE**

### **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 Five. 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.  
In specific cases a partner who has a power of prosecution e.g. Trading Standards Dept, Benefit Fraud Offices, will make requests for information. In these cases and where **there is a strong probability** that the information to be supplied will be presented at a Criminal Court hearing, the requesting partner may ask for the information to be provided in formal statement format, e.g. Police Statement MG11 format. In these cases the disclosing officer could be called to any subsequent court hearing, to answer questions relating to the information provided.
- 1.4 Each Form submitted in support of a request for Disclosure must be delivered by post or in person. Forms may only be submitted by fax in the event of an emergency 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.

#### **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 Form, a copy of which is attached at Appendix Five.
- 2.4 The Signatories should respond to formal requests for Disclosure of Personal Data within ten (10) working days of receipt of the request. However, it is acknowledged that there may be occasions when the Disclosure is required more urgently. In such circumstances, 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;

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 five (5) working days. In an emergency

situation, 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 Contact Officer identified in Appendix Two Part I.

**APPENDIX FOUR**

**REQUEST FOR DISCLOSURE OF PERSONAL DATA FORM**

|   |                             |                |  |
|---|-----------------------------|----------------|--|
| Headed paper of requesting Signatory – with name, address and contact information.  |                             |                |  |
| <b>CONFIDENTIAL</b><br><b>Crime and Disorder Act 1998</b><br><b>Devon and Cornwall Partnership Protocol for Crime and Disorder</b><br><b>Data Protection Act 1998</b><br><br><b>Request For Personal Data</b> |                             |                |  |
| I am making specific enquiries into matters covered by the Crime and Disorder Act 1998 under Section 17 and require personal information about:   |                             |                |  |
| <b>Our Reference:</b>   |                             |                |  |
| Surname:  | All forenames:              |                |  |
| All previous surnames(if applicable):   |                             |                |  |
| Also Known As/Alias:  | Place of Birth (if known) : |                |  |
| Sex: M/F  |                             |                |  |
| Date of Birth:  |                             |                |  |
| Present Address:<br>(with postcode)   |                             |                |  |
| Previous Address:<br>(with postcode)  |                             |                |  |
| The information I require is:   |                             |                |  |
|   |                             |                |  |
| I confirm that the personal data requested is required for the purpose indicated below and failure to provide the information will, in my view, be likely to directly prejudice that purpose.                 |                             |                |  |
| Signed:   |                             | Date           |  |
| Name (Capitals)   |                             | Rank/Job Title |  |

| Purpose(s) For Which Information Is Required:-Provision of this information will have the assumed effect of success in the pursuance of:  | Tick |
|---|------|
| Anti Social Behaviour Order(s)  |      |
| Sex Offender Order(s)   |      |
| Parenting Order(s)  |      |
| Child Safety Order(s)   |      |
| Reparation Orders   |      |
| Action Plan Orders  |      |
| Other Orders (please specify):-   |      |
| Or Any Other Activity – please specify:-  |      |
| <p>Failure to provide the information could jeopardise the following Crime reduction objective:</p> <ul style="list-style-type: none"> <li>(a) crime prevention;</li> <li>(b) crime detection;</li> <li>(c) Apprehension of offenders;</li> <li>(d) prosecution of offenders;</li> <li>(e) assessment of collection of any tax or duty;</li> </ul> <p>Because:-</p> |      |

**APPENDIX 5**

**DISCLOSURE OF PERSONAL DATA FORM**

Headed paper of requesting Signatory – with name, address and contact information.

**CONFIDENTIAL**  
**Crime and Disorder Act 1998**  
**Devon and Cornwall Partnership Protocol for Crime and Disorder**  
**Data Protection Act 1998**  
  
**Disclosure of Personal Data**

**To:**

**Your Reference:**

Further to your written request dated.....the information you have requested about:

(Full Name).....

Address: .....

is as follows:

|        |  |      |  |
|--------|--|------|--|
| Signed |  | Date |  |
| Name   |  |      |  |

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

- (i) the data must only be used for the specific purpose(s) for which it was requested;
- (ii) the data must be retained securely and in accordance with the standards included in the protocol

you will destroy the data when it ceases to be required for the specific purpose for which it was requested.

## **APPENDIX SIX**

### **Restrictions on the Disclosure of Personal Data**

1. The Signatories acknowledge that details of victims, witnesses or complainants must not be disclosed without their written consent.
2. Disclosures relating to cautions [refer to legislation issued under] will be made by the Devon and Cornwall Constabulary for a period of twelve (12) months after acceptance of the same. Details of cautions [refer to legislation issued under] (or reprimands/warnings issued under the Crime and Disorder Act 1998) which relate to an adult will not generally be the subject of a Disclosure as the Signatories acknowledge that the cautioning procedure creates an expectation that the offence has been dealt with and that no further action will be taken.
3. Devon and Cornwall Constabulary will allow Disclosure of warnings given pursuant to the Protection from Harassment Act 1997 in the event that two (2) or more warnings have been given in a period of twelve (12) months.
4. The Signatories understand that the exchange of Personal Data post conviction will be subject to a presumption of confidentiality but that this may be overridden on the grounds of public interest, as described in clause 5.10

## APPENDIX SEVEN

### PROCEDURES FOR HANDLING SUBJECT ACCESS REQUESTS

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. 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:
  - 2.1 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.
  - 2.2 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.
  - 2.3 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 Subject Access Requests 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 EIGHT

### DISCLOSABLE DATA

Information Disclosures. The following section details the information that the various signatories will disclose. Ownership of information of any type indicated in the lists will not indicate disclosures will always be made. **All requests will be treated on a case by case basis and considered in relation to the data subject's rights under Article 8 of the HRA and Proportionality and the Common Law Duty of Confidentiality.** Whilst the main power or disclosure in each case is listed, disclosures can also be empowered by the exemptions under the Data Protection Act 1998 and the Common Law Duty of Confidentiality.

#### **DEVON & CORNWALL CONSTABULARY will, where justified, disclose;**

1. Depersonalised data relating to crime or anti-social behaviour in the areas of housing owned or managed by the requesting signatory. Except where justified by a request citing a specific requirement of disclosure to a greater level of detail, this information will be supplied to postcode level, providing there are at least five houses within the postcode. Such information will only be disclosed on the understanding that the user will not merge the supplied data with other data sets to develop Personal Data from this source.
2. Evidence relating to a convictions for arrestable criminal offences providing the offence is not considered 'Stepped Down' under the ACPO Retention Guidelines of Records held on PNC. This Disclosure is empowered by the Crime & Disorder Act 1998.
3. Evidence relating to a cautions accepted for arrestable criminal offences, providing the offence is not considered 'Stepped Down' under the ACPO Retention Guidelines of Records held on PNC, empowered by the Crime & Disorder Act 1998 and in line with Force Policy.
4. Evidence of Warnings Given under the Protection from Harassment Act 1997, where warnings are recorded by the police within a period of twelve months empowered by the Protection from Harassment Act 1997, and in line with Force Policy. This Policy requires that there should be at least two occasions on which harassment has taken place, supported by substantive evidence, before an official warning is issued
5. Evidence from police records of incidents of anti-social behaviour. This Disclosure is empowered by the Crime and Disorder Act 1998.
6. Copies of statements made to the police by third parties relating to evidence in 2 – 5 above, where written permission had been provided by the statement maker for the statements disclosure for use in civil proceedings.

#### **The Local Authorities will disclose;**

1. Evidence, including complaints from neighbours or the public relating to criminal, immoral or anti social behaviour. This disclosure is empowered by the Crime and Disorder Act.
2. Additional detailed agreement on disclosures from individual Local Authority partners are as follows;

## **CARRICK DISTRICT COUNCIL**

The Council would disclose such data as may be disclosed pursuant to the Data Protection Act 1998 for the purposes of the prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of any duty or of any imposition of a similar nature.

## **EXETER CITY COUNCIL'S DATA**

Exeter City Council is committed to sharing information wherever the relevant legal provisions are satisfied. The following list is indicative of the types of information that the council holds and is neither exhaustive nor a commitment that the listed information will be disclosed in all situations.

The council holds information about current, past and potential:

- Employees
  - Councillors
  - Trainers
  - Contractors
  - Volunteers who work with the council
  - Benefit claimants
  - License applicants e.g. taxis; entertainment
  - Businesses including our business tenants
  - Grant applicants
  - Residents and council tax payers
  - Council owned housing tenants and leaseholders
  - Homelessness applicants
  - Leisure facility users including allotment holders
  - Market traders
  - Hall users
  - Parking permit holders
  - Planning and building control applicants
  - Council tax and NNDR payers
  - Concessionary bus pass holders
  - CCTV footage e.g. from the city centre and car parks (currently administered by Devon County Council but new control centre planned)
- Electoral role entries
- .