

Information Sharing Protocol

The Devon Children's Trust is a partnership between social care, education, health, community, voluntary and justice services working together to make a difference for Devon's children and young people.

Parties signed up to the Protocol

Parties	Signatories
Connexions Cornwall & Devon Ltd	Jenny Rudge Chief Executive
Devon & Cornwall Constabulary	Mr R Pennington ACC (Operations)
Devon County Council	Anne Whiteley Executive Director, Children and Young People's Services
Devon Primary Care Trust	Virginia Pearson Caldicott Guardian
Devon and Cornwall Probation Area	Mary Mitchell Assistant Chief Officer
Devon Youth Offending Service (YOS)	Martin Spragg YOS Manager
Northern Devon Healthcare NHS Trust	Dr Alison Diamond Associate Medical Director
Royal Devon & Exeter NHS Foundation Trust	Vaughan Pearce Joint Medical Director and Caldicott Guardian
South Devon Healthcare NHS Trust	Paul Stannard Caldicott Guardian
South Western Ambulance Services NHS Trust	Ken Wenman Chief Executive

1. Purpose

This Protocol provides a framework for sharing children and young people's information.

The recommendations set out in the *Integrated Children's Services Framework* (sponsored by the Communities and Local Government's ROAD Programme) have been considered when creating this Protocol.

The purpose of this Protocol is to enable the sharing of information (including personal data) between the signatories, in furtherance of their statutory duties.

2. Definitions and interpretations

All defined terms used throughout this Protocol are described in the glossary.

3. Core objectives and standards

The signatories, when preparing this Protocol, subscribe to the core objectives and standards and agree that any amendments to the Protocol will also subscribe to the core objectives and standards.

The core objectives and standards mean that:

- 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
- the Protocol must set out the legal basis for the exchange of the information it covers
- for all exchanges of information *The Data Protection Act (DPA) 1998*, and in particular the Data Protection Principles set out in Schedule 1 of the DPA 1998, should be upheld
- the common law principles of confidentiality should be upheld
- the rights of the data subjects and other individuals under *The Human Rights Act 1998* should be upheld
- the Protocol should be reviewed regularly (see section 23) and in the light of new legislation and official guidance
- 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.

4. Law governing and enabling the sharing of personal data under this Protocol

Legal power to make disclosures

The signatories may each only make disclosures if 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 (see Appendix Two) and for sensitive personal data one of the conditions set out in Schedule 3 of the DPA 1998, must also be met (see Appendix Three).

The Signatories acknowledge that they may be legally empowered under any of the sections of the Acts set out below.

Children's Act 1989

[Section 17](#) - general duty of local authorities to safeguard and promote the welfare of children within their area who are in need, and so far as is consistent with that duty, to promote the upbringing of such children by their families.

[Section 47](#) - where a local authority is informed that a child who lives, or is found, in their area is the subject of an emergency protection order or is in police protection or there is reasonable cause to suspect that a child who lives, or is found, in their area is suffering, or is likely to suffer, significant harm, there is a duty to investigate.

Children's Act 2004

[Section 10](#) - promote co-operation to improve wellbeing.

[Section 11](#) - arrangements to safeguard and promote welfare.

Children (Leaving Care) Act 2000

[Section 24C\(1\)](#) - where it appears to a local authority that a person with whom they are under a duty to keep in touch under section 23B, 23C or 24; or whom they have been advising and befriending under section 24A; or to whom they have been giving assistance under section 24B, proposes to live, or is living, in the area of another local authority, they must inform that other authority.

[Section 24C\(2\)](#) - where a child who is accommodated by a voluntary organisation or in a private children's home, by any Health Authority, Special Health Authority, Primary Care Trust or local education authority or in any care home or independent hospital or any accommodation provided by a National Health Service trust, ceases to be so accommodated, after reaching the age of sixteen, the organisation, authority or (as the case may be) person carrying on the home shall inform the local authority within whose area the child proposes to live.

Crime and Disorder Act 1998

[Section 17](#) - duty of each authority to exercise its functions with due regard to the likely effect of the exercise of those functions, and the need to do all that it reasonably can, to prevent crime and disorder in its area.

[Section 115](#) - any person who apart from this section would not have power to disclose information to a relevant authority or to a person acting on behalf of such an authority, shall have power to do so in any case where the disclosure is necessary or expedient for the purposes of this Act.

Criminal Justice and Courts Services Act 2000

Section 67 - the authority for each area must establish arrangements for the purpose of assessing and managing the risks posed in that area by relevant sexual or violent offenders and other persons who have committed offences who are considered by the authority to be persons who may cause serious harm to the public.

Section 68 - interpretation of who is a relevant sexual or violent offender.

Data Protection Act (DPA) 1998

Section 29(3) - where disclosure is required for the prevention or detection of crime or the apprehension or prosecution of offenders.

Section 34 - where a data controller is obliged by or under any enactment to make personal data available to the public.

Section 35(1) - where the disclosure is required by or under enactment, by any rule of law or by the order of a Court.

Section 35(2) - where the disclosure is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) or for the purpose of obtaining legal advice or establishing, exercising or defending legal rights.

Education Act 1996

Section 322 - where it appears to a local education authority that any health authority or local authority could, by taking any specified action, help in the exercise of any of their functions under this Part, they may request the help of the authority, specifying the action in question.

Education Act 2002

Section 175 - A local education authority shall make arrangements for ensuring that the functions conferred on them in their capacity as a local education authority are exercised with a view to safeguarding and promoting the welfare of children.

Health and Social Care Act 2001

Section 60 - gives the Secretary of State for Health powers to authorise use of identifiable information for essential medical purposes without the consent of patients.

Learning and Skills Act 2000

Section 114 - the Secretary of State may provide or secure the provision of services which he thinks will encourage, enable or assist the effective participation by young persons in education or training. In securing the provision of those services the Secretary of State may make arrangements with local authorities and other persons for the provision of services.

Section 120 – for the purpose of the provision of services in pursuance of section 114, any of the persons or bodies mentioned may supply information about a young person (a person who has attained the age of 13 but not the age of 20) to the Secretary of State or to any other person or body involved in the provision of those services. Those persons and bodies are a local authority, a health authority, the Learning and Skills Council for England, a chief officer of Police, a probation committee, a youth offending team and a Primary Care Trust.

Local Government Act 2000

Section 2 – councils have the power to do anything which is considered likely to achieve any one or more of their objectives.

- To promote or improve the economic wellbeing of their area.
- To promote or improve the social wellbeing of their area.
- To promote or improve the environmental wellbeing of their area.

Management of Police Information (MOPI)

Code of Practice on the Management of Police Information.

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.

Policing purposes are defined in the code as:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice
- any duty or responsibility of the Police arising from common or statute law.

The code allows the police to disclose police information to the other people or bodies where this is reasonable and lawful to do for the policing purposes as set out in Sub paragraph 2. Any sharing of information must comply with the ACPO Guidance on the Management of Police Information 2006 and any protocol, local or national, which may be agreed with the people or bodies needing to receive the information.

Additionally the code of practice sets out obligations on the people or bodies receiving police information which equate to the requirements set out in sections 7, 12, 16, 17, 18, 19 and 20 of this Protocol.

National Health Service Act 1977

Section 22 – in exercising their respective functions health and local authorities shall co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.

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

The signatories shall each take into account and comply with all legal requirements. In the case of personal data held under a duty of confidence, a disclosure may be made in respect of that personal data, if the public interest demands it or there is another overriding statutory justification which permits the disclosure. For the purposes of public interest, the signatories understand the public interest criteria to include, but not limited to:

- the protection of children from harm as a result of abuse or neglect
- the prevention or detection of crime
- the apprehension of offenders
- order of court, or for taxation or public health issues.

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

- is the intended disclosure proportionate to the intended aim?
- how vulnerable are those at risk?
- is there another equally effective means of achieving the same aim?
- is the disclosure necessary to prevent or detect crime and uphold the rights and freedoms of the public?
- is the disclosure necessary to protect other vulnerable people?

The signatories acknowledge that the duty of confidentiality can extend to information relating to deceased individuals and that duty must be upheld. The Access to Health Records Act 1990 gives some eligible people the right to access Health Records of deceased individuals.

The signatories recognise that Article 8 of the *Human Rights Act 1998* states that everyone has the right to respect for his or her private and family life, home and his or her correspondence. 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:

- national security
- public safety
- economic wellbeing of the country
- the prevention of crime and disorder
- the protection of health and morals, or
- the protection of the rights or freedoms of others

and shall apply the same when considering and making disclosures.

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 Protocol. In the event of any conflict between such guidance and the relevant Act(s) or laws, then the Act(s) or laws will prevail.

This list of Acts and sections is not exhaustive. It is intended to be a point of reference, signatories should read the relevant sections within the Acts themselves if wishing to rely on them, when requesting or disclosing personal information.

5. Caldicott Principles

All health and social care organisations have a Caldicott Guardian to oversee access to patient and service user information. Health and social care signatories agree to access, share and disclose patient-identifiable information in accordance with the six Caldicott principles.

- 1. Justify the purpose(s) for using confidential information.**
- 2. Only use it when absolutely necessary.**
- 3. Use the minimum that is required.**
- 4. Access should be on a strict need-to-know basis.**
- 5. Everyone must understand his or her responsibilities.**
- 6. Understand and comply with the law.**
- 6. Requests for the disclosure of anonymous information**

6. Requests for the disclosure of de-personalised information

This Protocol is primarily concerned with the exchange of personal data between all Signatories. The Signatories agree that disclosures of personal data will not be made under this Protocol where a disclosure of de-personalised (anonymous) data would suffice. For example, de-personalised aggregated or statistical data may be disclosed instead.

If a Signatory requests that another Signatory discloses de-personalised data, the signatory receiving the request shall make the disclosure requested, subject to the following conditions:

- the de-personalised data will only be used for the purpose for which it is requested
- the de-personalised data will not be processed in such a way that information about a living individual may be extracted from the data.

7. Legality of disclosure

Each of the signatories acknowledges responsibility for ensuring and satisfying themselves that it is permitted by law to disclose personal data to another signatory to this Protocol.

8. Sharing information with other signatories

The signatories agree to adhere to the Devon Children's Information Sharing Protocol - Practitioners' Guide when sharing information with other signatories. This guide is supplementary to the Protocol.

9. Future Information Sharing Agreements

The signatories agree that any arrangements for sharing information about children, young people or their families for specific purposes, will be made as an Information Sharing Agreement (see Template, Appendix Five) which will sit under this Protocol.

The signatories agree that the contact officer will be informed of any new Information Sharing Agreement and that each new Information Sharing Agreement will be signed by the relevant signatories under this Protocol.

10. Sharing information with organisations not listed in this Protocol

If a signatory is asked to disclose information about a child or young person or their family, to an organisation or person not signed up to this Protocol, information can be shared provided the disclosure is lawful.

A disclosure may be considered lawful if at least one of the following conditions apply:

- legislation permits the disclosure
- a court order demands the disclosure to be made
- consent has been obtained from the person the information is about, or from an appropriate person who is eligible to consent on that person's behalf
- the disclosure is in the public interest
- the disclosure is in the vital interests of an individual - for example, if it is necessary for matters of life and death or for the prevention of serious harm to the individual.

Disclosures made to any organisation must be recorded and include a reason for the disclosure or if refused, the reason why the information was not disclosed.

11. Consent

Signatories must obtain consent from the data subject or their parent or legal guardian or both before requesting or sharing the data subject's personal data with other signatories, unless this would be contrary to the need to safeguard the child or young person's welfare.

For example, if the information is needed urgently, the delay in obtaining consent may not be justified. Consent should not be sought if it is thought that it might prejudice a police investigation or increase the risk of harm to the child or young person.

12. 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 procedures and policies
- the relevant policies of any professional or regulatory bodies which govern the work of the signatory when making a disclosure.

To this end, each signatory shall obtain their own legal advice where necessary.

13. 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, and where appropriate, be as generalised as possible. This will be determined on a case by case basis.

14. Proportionality

The signatories agree that if a disclosure will in some way restrict the rights of the relevant data subject, the relevant signatory(s) will have regard to the need for 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.

15. Partnership contact officers

Each of the signatories will nominate a contact officer who will be the main point of contact for their organisation in respect of this Protocol. The signatory shall remain the Chief Knowledge Officer. The nominated contact officers are identified in Appendix One.

The relevant contact officer shall be the point of contact for each signatory, without limitation:

- for any other signatory requesting a disclosure or other request for relevant information from it
- to whom disclosures may be made.

Information requests and disclosures may be dealt with by individuals in the contact officer's organisation, unless agreed otherwise. When this is the case, it is the responsibility of the contact officer to ensure that any disclosures made are in accordance with the law and the best practice recommendations set out in the Devon Children's Information Sharing Protocol – Practitioners' Guide (supplementary to this Protocol).

Decision-making flowchart

This will involve training all staff who might receive requests as part of this Protocol and ensuring that they understand their legal limitations when requesting information and making disclosures. Staff should not be permitted to request information, or make any disclosures in relation to this Protocol, until they have received appropriate training. Signatories recognise the benefits of keeping a record of staff who have been trained and are authorised to process information and make disclosures in relation to this Protocol.

Any change in a contact 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.

16. Registration and notification under DPA 1998

Each signatory will ensure that, at all times, they are appropriately registered under the DPA 1998 to receive, disclose and otherwise process Personal Data in accordance with this Protocol.

17. Accuracy of data

The signatories acknowledge their responsibility to verify and maintain the accuracy of personal data subject to this Protocol, which is held by them. This is a statutory duty set out in Schedule One of the DPA 1998.

Where an inaccuracy is discovered after a disclosure has been made, it is the responsibility of the signatory discovering the inaccuracy to notify the signatory making the disclosure, in writing. The signatory making the disclosure will notify all other signatories who have also received the data of the inaccuracy and any correction required.

To meet these obligations, signatories are expected to record all disclosures made, including the reasons why, when and to whom the information was disclosed.

18. Use of personal data and confidentiality

Process in accordance with purpose

Signatories must only use personal data, received by means of a disclosure, in accordance with the purpose of this agreement and the guidance set out in the Devon Children's Information Sharing Protocol - Practitioners' Guide.

Confidentiality

Signatories may only publish personal data disclosed to them by another signatory under this Protocol if the data has been de-personalised and is anonymous.

Disclosure of personal data to another signatory

To avoid any doubt, a signatory who receives personal data through disclosure by another signatory, must not disclose that personal data to another signatory without the consent of the original signatory or by obtaining consent directly from the relevant data subject, unless otherwise required by law.

Section 18 shall survive termination of the Protocol or the withdrawal of, or removal of, any signatory.

19. Security

Each signatory will take all reasonable steps to adequately protect the personal data received from another signatory, from unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, that data.

Each signatory must ensure that access to personal data and other information obtained from another signatory under this Protocol by individuals employed or engaged by that signatory will be restricted to individuals who need the information to do their job.

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

The signatories will endeavour to adopt National standard BS7799 for making data (including personal data, de-personalised data and other data) secure, in accordance with their respective internal policies and procedures.

The provision of section 19 will survive termination of the Protocol or the withdrawal, or removal of any signatory.

20. Retention and disposal of personal data

The signatories acknowledge that Schedule One of the DPA 1998 provides that personal data excessive to the purpose for which they are processed must not be retained.

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. signatories are expected to introduce a procedure and nominate a person to conduct regular (at least six monthly) reviews of personal data received through disclosure.

21. Subject Access Requests

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

Signatories agree that they will 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 wholly or partly to personal data received from signatories through a disclosure, the signatory receiving the Subject Access Request will also apply the Procedure for Handling Subject Access Requests set out in Appendix Four.

The signatories recognise that the DPA 1998 does not cover data relating to deceased people. Where a request is received from third parties for access to data relating to deceased people, it should not be treated in the same manner as a Subject Access Request. Such data will be dealt with according to their own internal procedures in consultation with other signatories where appropriate in the event of the data originating from the other signatories.

22. Complaints

All complaints made in respect of disclosures or other matters relating to this Protocol will be brought to the attention of the nominated contact officer of the relevant signatory, by the signatory receiving the complaint. The complaint will be dealt with in accordance with the relevant internal policies and procedures of the relevant signatory.

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

23. Regular review of the Protocol and consultation about the Protocol

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

- within the first six months of the date of the Protocol being signed
- on an annual basis after that
- in the event that any new legislation comes into force or official guidance is issued which impacts on the Protocol or the obligations of any or all of the signatories under the Protocol.

24. Changes to the Protocol

Signatories can ask for any changes to the Protocol at any time by submitting a request to the nominated holder who will:

- circulate the requests to all signatories
- co-ordinate responses, and where appropriate,
- seek the agreement to the requested changes from the signatories.

No change can be made to the Protocol without the agreement of all the signatories being recorded in writing.

25. Changes to signatories

Any signatory may withdraw from being a signatory to this Protocol after giving written notice to the other signatories and notifying the nominated holder in writing. If a signatory breaches a term of this Protocol (or persistently breaches the terms), the other signatories may, upon a majority vote, remove that signatory's status as a signatory.

All personal data received by means of disclosures from other signatories must be returned or destroyed if a signatory withdraws or is removed from this Protocol. 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.

26. Indemnity

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 agents, or any of the provisions of this 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.

27. Publication of the Protocol

This Protocol may be published by each of the signatories in accordance with their respective obligations under the Freedom of Information Act 2000.

Glossary

Data controller

a person who either alone or jointly with other people, determines the purposes for which any personal data are to be processed.

Data subject

a person who is the subject of personal data.

De-personalised data

any information where any reference to or means of identifying a living individual has been removed.

Disclosure

a disclosure by one signatory to any other signatory of personal data.

DPA 1998

Data Protection Act 1998.

Nominated holder

the nominated holder of this Protocol – this is currently the Information Compliance Officer for Devon County Council.

Contact officers

all those individuals identified in Appendix One.

Chief Knowledge Officer

the individual signing this Protocol.

Personal data

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 any expression of opinion or intentions in respect of the living individual.

Processing

obtaining, recording or holding personal data or carrying out any operation or set of operations on the information or data including:

- organisation, adaptation or alteration of the personal data
- retrieval, consultation or use of the personal data
- disclosure of the personal data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the personal data.

Protocol

this Protocol.

Purpose

the purpose of this Protocol.

Sensitive personal data

see categories of sensitive personal data in Appendix Three.

Signatories

the signatories or parties to this Protocol.

Subject Access Request

a request made by a data subject to a signatory pursuant to section 7 of the DPA 1998.

Schedule 1 – DPA 1998 the Data Protection Principles:

1. Personal data shall be processed fairly and lawfully and in particular shall not be processed unless:
 - a) at least one of the conditions in Schedule 2 is met, and
 - b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and where possible kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appendix One

Contact information for partnership contact officers

Organisation	Name or post of contact officer (CO)	Contact details
Connexions Cornwall & Devon	John Davey Director of Service Delivery (Devon and Torbay)	01392 203603 37-39 Queen Street, Exeter, EX4 3SR john.davey@connexions-cd.org.uk
Devon & Cornwall Constabulary	John Ellis Force Information Manager and Interim PCO	01392 452903 Devon & Cornwall Constabulary, Force HQ, Middlemoor, Exeter, EX27HQ john.ELLIS@devonandcornwall.pnn.police.uk
Devon County Council	Richard Stevens Information and Data Manager, Children and Young People's Services	01392 382034 Room 142, County Hall, Topsham Road, Exeter, EX2 4QG richard.stevens@devon.gov.uk
Devon Primary Care Trust	Information Governance Manager	01392 205205 Devon Primary Care Trust, Dean Clarke House, Southernhay East, Exeter, EX1 1PQ foi.devonpct@nhs.net
Devon and Cornwall Probation Area	Mary Mitchell Assistant Chief Officer	01392 421122 or 07855 267968 3/5 Barnfield Road, Exeter EX1 1RD mary.mitchell@devon-cornwall.probation.gsi.gov.uk
Devon Youth Offending Service (YOS)	Martin Spragg YOS Manager	01392 384963 Ivybank, 45 St David's Hill, Exeter, EX4 4DN martin.spragg@devon.gov.uk

<p>Northern Devon Healthcare NHS Trust</p>	<p>David Lawrence Information Governance Lead</p>	<p>01271 311682 Suite 8, Munro House, North Devon District Hospital, Barnstaple, EX31 4JB david.lawrence@ndevon.swest.nhs.uk</p>
<p>Royal Devon & Exeter NHS Foundation Trust</p>	<p>Sharon Collingwood Information Governance Manager</p>	<p>01392 402261 Royal Devon and Exeter Hospital, Barrack Road, Exeter, EX2 5DW sharon.martin@rdefn.nhs.uk</p>
<p>South Devon Healthcare NHS Trust</p>	<p>Lucy Beckwith Operational Manager, Child Health</p>	<p>01803 655288 or 07771 912540 Hengrave House, Torbay Hospital, Newton Road, Torquay, TQ2 7AA lucy.beckwith@nhs.net</p>
<p>South Western Ambulance Services NHS Trust</p>	<p>Safeguarding Lead</p>	<p>01392 261657 Westcountry House, Unit 3 Abbey Court, Eagle Way, Sowton Industrial Estate, Exeter, EX2 7HY publicrelations@swast.nhs.uk</p>

Appendix Two

Schedule 2 of the Data Protection Act

Conditions relevant for purposes of the first principle: processing of 'any' Personal Data.

1. The Data Subject has given consent to the processing.
2. The processing is necessary:
 - a) for the performance of a contract to which the Data Subject is a party, or
 - b) for the taking of steps at the request of the Data Subject with a view to entering into a contract.
3. The processing is necessary for compliance with any legal obligation to which the Data Controller is subject, other than an obligation imposed by contract.
4. The processing is necessary in order to protect the vital interests of the Data Subject.
5. The processing is necessary:
 - a) for the administration of justice
 - b) for the exercise of any functions conferred on any person by or under any enactment
 - c) for the exercise of any functions of the Crown, a Minister of the Crown of a government department, or
 - d) for the exercise of any other function of a public nature exercised in the public interest by any person.
6. The processing is necessary for the purposes of legitimate interests pursued by the Data Controller or by the third party or parties to whom the data is disclosed, except where the processing is unwarranted in any particular case by reason or prejudice to the rights and freedoms or legitimate interests of the Data Subject.

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

Appendix Three

Schedule 3 of the Data Protection Act

Conditions relevant for purposes of the first principle: Processing of Sensitive Personal Data.

1. The Data Subject has given explicit consent to the processing of the Personal Data.
2. (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the Data Controller in connection with employment.
(2) The Secretary of State may by order:
 - a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
3. The processing is necessary:
 - a) in order to protect the vital interests of 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 reasonably be expected to obtain the consent of the Data Subject, or
 - b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the Data Subject has been unreasonably withheld.
4. The processing:
 - a) is carried out in the course of its legitimate activities by any body or association which:
 - i) is not established or conducted for profit, and
 - ii) exists for political, philosophical, religious or trade-union purposes
 - b) is carried out with appropriate safeguards for the rights and freedoms of Data Subjects
 - c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
 - d) does not involve disclosure of the Personal Data to a third party without the consent of the Data Subject.
5. The information contained in the Personal Data has been made public as a result of steps deliberately taken by the Data Subject.
6. The processing:
 - a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
 - b) is necessary for the purpose of obtaining legal advice, or
 - c) 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 functions conferred on any person by or under an enactment, or
 - c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
(2) The Secretary of State may by order:
 - a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
 - b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8. (1) The processing is necessary for medical purposes and is undertaken by:
 - a) a health professional, or
 - b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.(2) In this paragraph 'medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
9. (1) The processing:
 - a) is of sensitive Data Subject consisting of information as to racial or ethnic origin
 - b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
 - c) is carried out with appropriate safeguards for the rights and freedoms of Data Subjects.(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of Data Subjects.
10. The Personal Data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.

The Data Protection Act defines categories of Sensitive Personal Data as:

'namely 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 committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.'

Data Protection Act 1998

Appendix Four

Procedures for handling Subject Access Requests

All Signatories should have internal procedures in place for handling and responding to Subject Access Requests - requests for access to Personal Data made pursuant to section 7 of the Data Protection Act 1998.

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 these requests.

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 Officer to determine whether they wish to claim an exemption to withhold the Personal Data under the provisions of the Data Protection Act.

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 to that Personal Data that information has been withheld.

Third party information

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 section 7 and 8 of the Data Protection Act 1998 shall govern whether or not the disclosure should be made.

Time limit for dealing with Subject Access Requests

Subject Access Requests must be dealt with as quickly as possible. Data Controllers have a statutory obligation to respond to Subject Access Requests within 40 calendar days, provided that sufficient information is received from the Data Subject.

Appendix Five

Template

Information Sharing Agreement

between

and

relating to

Version

Date

Disclosure checklists

Introduction

This is an agreement between

and

to share personal information for the purposes of

This agreement is supplementary to the overarching **Devon Children's Information Sharing Protocol** (the Protocol) and is supported by the **Devon Children's Information Sharing Protocol - Practitioners' Guide**.

It is not intended that this document will repeat the advice and guidance provided by the Protocol and the Practitioners' Guide but will highlight specific sharing agreements between the agencies stated above.

1. Law governing and enabling the sharing of personal data under this agreement

Act	Section
<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>

Other relevant information such as Home Office Circulars

2. Information to be shared under this agreement by

-
-
-
-
-

3. Action by

has agreed to provide the information stated above where the law permits disclosure.

will disclose this information in the following circumstances:

-
-
-
-
-

4. Information to be shared under this agreement by

-
-
-
-
-

5. Action by

has agreed to provide the information stated above where the law permits disclosure.

will disclose this information in the following circumstances:

-
-
-
-
-

6. Sharing personal information securely

Each of the signatories agree to follow the guidance on sharing information securely, outlined in the Devon Children's Information Sharing Practitioners' Guide.

7. Disclosure of Personal Data to another agency

Information provided by one agency must not be given to another agency or used for a different purpose without informing and obtaining the consent of the original provider or the subject of the information, unless an exemption applies.

8. Indemnity

Each of the signatories agree to comply with the indemnity statement provided in the Devon Children's Information Sharing Protocol.

9. Partnership contact officers

Name and job title	Organisation	Contact details

10. Review of this agreement

The nominated holder of this agreement is the Information Compliance Officer of Devon County Council who shall, on behalf of the partners, instigate a review of this document every months.

The next review date is

11. Certification of this agreement

By signing below, the signatories accept and agree to be bound by the provisions contained in the Devon Children’s Information Sharing Protocol Version 1 and this agreement.

Signed

By

Enter name and position of person signing

For and behalf of

Insert full name of organisation

Date

Data Protection Act 1998

Insert DPA Registration Number **Z** _ _ _ _ _

Appendix Six

Certification

Devon Children's Information Sharing Protocol

By signing below, the signatories accept and agree to be bound by the provisions contained in the Devon Children's Information Sharing Protocol Version 1.

Signed

By

Enter name and position of person signing

For and behalf of

Insert full name of organisation

Date

Data Protection Act 1998

Insert DPA Registration Number **Z** _ _ _ _ _

For more copies of this document email childrens.trust@devon.gov.uk

Find more information about the Devon Children's Trust at www.devonchildrenstrust.org.uk