

# Code of Practice for sharing children and young people's information





# Contents

1. Introduction
2. What is the Code of Practice and who is it for?
3. Laws enabling and governing the sharing of personal data
4. Consent and parental responsibility
5. Share minimum personal information
6. Information standards
7. Keeping information secure
8. Access to personal information
9. Complaints
10. Partnership Contact Officers
11. Working practice information sharing agreements
12. Code of Practice review and changes
13. Publication of Code of Practice
14. Children's Trust Information Sharing Forum

## **Appendix One**

Law enabling and governing the sharing of personal data

## **Appendix Two**

Checklists for sharing information under the DPA 1998

## **Appendix Three**

Checklist for sharing information securely

## **Appendix Four**

Partnership contact officers

## **Appendix Five**

Template working practice agreement

## **Appendix Six**

Useful sources of advice and guidance

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.

**[www.devonchildrenstrust.org.uk](http://www.devonchildrenstrust.org.uk)**

This document has been produced by Devon County Council;  
proud partner of Devon Children's Trust.

## 1. Introduction

This Code of Practice has been adopted by the Devon Children's Trust Partnership as good practice for sharing personal data about children and young people and their families. A list of the membership can be found on the website at [www.devonchildrenstrust.org.uk](http://www.devonchildrenstrust.org.uk)

Devon Children's Trust is a partnership of public and voluntary sector organisations working together to meet the needs of children and families. The Children's Trust exists to improve outcomes for children and young people because we believe that this can be done more effectively by all agencies and organisations working together. It is expected that all organisations working with the Trust who handle personal information about children and young people, will adhere to the law and the good practice recommendations of this Code when sharing personal data about children and young people.

## 2. What is the Code of Practice and who is it for?

Sharing information about individuals is often essential if we are to keep people safe, or ensure they get the best services they need. This Code of Practice is to provide a framework for sharing children and young people's information in Devon, which ensures that any sharing that takes place, is necessary, proportionate, relevant, accurate, secure and timely.

This Code of Practice applies to all Children's Trust partners and their staff who make decisions about sharing personal information. These are referred to as 'partners' throughout the Code of Practice.

The code also applies to organisations commissioned to process personal information by Childrens Trust partners.

**Appendix Six** provides a list of useful sources of advice and guidance about information sharing and should be read alongside this Code of Practice.



### 3. Laws enabling and governing the sharing of personal data

There are many laws that enable and govern information to be shared about children and young people. This Code of Practice provides a list of the most relevant Acts which give either a 'duty to share' or a 'power to share' personal information. These can be found in **Appendix One**. The list is not exhaustive.

Partners are reminded that when sharing information under the legislation listed in **Appendix One**, they must still take into account their legal obligations under the Data Protection Act 1998, *Human Rights Act 1998* and the Common-Law Duty of Confidentiality. Health and social care organisations may also take into account the non-statutory NHS Caldicott Principles, which govern the handling of patient-identifiable information.

#### Data Protection Act 1998

The Data Protection Act 1998 (DPA 1998) is the legal framework for obtaining, using, storing, disclosing and deleting personal data about living and identifiable people. The Act is built around eight 'common-sense' principles.

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be processed for limited purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data shall be kept for no longer than is necessary.
6. Personal data shall be processed in line with the individual's rights.

7. Personal data shall be kept secure.
8. Personal data shall not be transferred to countries without adequate security.

Partners that process personal information about children and young people must comply with these principles, in particular Principle One, which is about processing information fairly and lawfully.

#### Fair and lawful processing

In order for sharing to be fair, the individual the information is about (the data subject) should be told (either in writing or verbally) who their information is going to be shared with and why, and give them the opportunity to object, where this is appropriate. This is known as a 'privacy notice' or a 'fair processing notice'. Partners will follow the Information Commissioner's guidance on drafting privacy notices and will adhere to their own procedures for issuing them to data subjects.

For the sharing of personal information to be considered lawful, the disclosing partner must be able to satisfy one or more conditions listed in Schedule 2 of the DPA 1998 and in the case of sharing sensitive personal data, one or more conditions in Schedule 3 of the DPA 1998 as well.

The DPA 1998 lists the type of information that it considers is 'sensitive personal data'. For example, information about a person's racial or ethnic origin; religious or other beliefs; physical or mental health or condition; sexual life; whether the person has been accused of an offence or committed an offence (including the outcome of the proceedings).

**Appendix Two** provides two checklists to help partners decide whether they can share personal information lawfully, under principle one of the DPA 1998. Partners acknowledge that they must also consider the other

principles, when deciding whether or not they can share information.

### **Human Rights Act 1998**

When sharing personal information, partners must respect the individual's rights under the Human Rights Act 1998 (the HRA). The HRA gives effect in UK law, the rights contained in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Article 8 of the ECHR is of particular importance when using and sharing personal information. Article 8 is divided into two parts.

The first part (Article 8, paragraph one) sets out the precise rights which are to be guaranteed to an individual by the State, that is to say, the right to respect for private and family life, home and correspondence.

The second part (Article 8, paragraph two) makes it clear that those rights are not absolute in that it may be acceptable for public authorities to interfere with the Article 8 rights in certain circumstances. Interference with a person's Article 8 rights can be made provided it is in accordance with the law and necessary in a democratic society in pursuit of one or more of the legitimate aims.

The legitimate aims are listed as national security; public safety or the economic wellbeing of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the rights and freedoms of others.

### **Proportionality**

If a partner wants to share personal information about a child or young person and it is not appropriate or necessary to obtain the child or their parent's consent, they must ensure that their disclosure is lawful and their actions are proportionate to the aim of the disclosure.

In determining whether the disclosure is proportionate, the partner must decide whether the public interest in making the disclosure outweighs the right to a private life of the child or a third party. The information shared must be adequate, relevant and not excessive for the purpose of the disclosure.

### **Common-Law Duty of Confidentiality**

There may be times when a partner wants to share information which was originally provided in confidence. Case law has surmised confidential information as something that has the "necessary quality of confidence about it" (*Saltman Engineering Company v Campbell Engineering Company Ltd* (1948) 65 RPC 203) and is not something that is public knowledge.

A duty of confidence will generally arise in circumstances where a person receives information that they know, or ought to know, is being given in confidence. In such cases the partner or person given the information, is restricted from using it for a purpose other than that for which it was provided, or disclosing it without the individual's permission, unless there is some overriding reason in the public interest for this to happen or another law or power permits disclosure.

When deciding whether there is a public interest in sharing confidential information, partners agree to consider the following questions.

- Do we have the person's consent?
- Is the sharing necessary to protect a child or young person from harm as a result of abuse or neglect?
- Is the sharing necessary to prevent or detect crime?

- Is the sharing necessary to apprehend an offender?
- Is the sharing necessary to comply with a court order or a legal obligation?

When deciding if the public interest should override a duty of confidence, Partners also agree to consider the following questions.

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

Partners recognise that the duty of confidentiality can also 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.

## 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 partners 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 their responsibilities.
6. Understand and comply with the law.



## 4. Consent and parental responsibility

If a partner is relying on consent as their lawful power to share personal information, they must make sure the person giving consent is 'fully informed'. This means the person must understand why their information may be shared, who will see their information and any implications that may result from the sharing or indeed not sharing the information.

Partners recognise the approach to obtaining consent must be transparent and should respect the individual. Consent must be freely given and must not be obtained through coercion or inferred from a lack of response to a request for consent. The person giving consent (child or person with parental responsibility) must be capable of taking that particular decision; acting voluntarily and not under pressure or duress from anyone; and provided with enough information to enable them to make the decision.

### Whose consent should be sought?

Partners recognise that where a child is under 12 years old, consent should be sought from the parent (or other person with parental responsibilities). Where a child is over 12 but under 16 years old, Partners will assess whether the child is competent to consent for themselves. If they are assessed as being competent, Partners will seek consent directly from them.

Partners recognise that young people over 16 years old are usually considered competent to give consent and therefore consent will be obtained from them direct. However, partners understand that even if a young person is over 16 there may be issues, as with adults, that affect their capacity to consent.

Partners recognise that it is good practice to encourage competent children to involve their families in decision-making, unless this is not in their best interests to do so.

### Establishing competence

When establishing whether a child or young person is competent to give consent, Partners agree to consider the following questions.

- Does the child understand the question being asked of them?
- Does the child have a reasonable understanding of what information might be shared; the main reasons for sharing the information and the implications of sharing that information and of not sharing it?
- Can the child or young person express their own opinion on the matter and not just repeat what someone else thinks they should do?
- Can the child or young person fully understand the implications of their decision?

### Parental responsibility

If a child is not competent to give consent for themselves, partners will seek consent (where appropriate) from a person with parental responsibility. This will often be, but is not always, the child's parent.

Consent is only required from one person with parental responsibility, although partners acknowledge it is good practice to involve all those close to the child in the decision-making process.

Partners recognise that in England and Wales, if the parents of a child are married to each other at the time of the birth, or if they have jointly adopted a child, then they both have

parental responsibility. Partners also recognise that parents do not lose parental responsibility if they divorce and this applies to both the resident and the non-resident parent.

According to current law, a mother always has parental responsibility for her child. A father however, has this responsibility only if he is married to the mother when the child is born or has acquired legal responsibility for his child through:

- jointly registering the birth of the child with the mother (from 1 December 2003)
- a parental responsibility agreement with the mother
- a parental responsibility order, made by the court

A person also has parental responsibility if they have been appointed as a guardian, by a Court or by the mother or other guardian; are a person in who a court has made a residence order concerning the child; are a local authority designated in a care order in respect of the child (but not where the child is being looked after under Section 20 of the Children Act 1989) or are a local authority or other authorised person who holds an emergency protection order in respect of the child.

### Objection to sharing

Partners agree that if a child, young person or someone with parental responsibility for them, objects to their information being shared this should, where appropriate, be upheld. However, partners recognise that there may be times when they should override a refusal of consent or not seek consent in the first place, in cases where the sharing is necessary to protect a child or young person from harm or assist in the prevention or detection of a crime.

In such cases, there may be other laws that will allow the partners to share the information without consent (see **Appendix One** and **Two**).



## 5. Share minimum personal information

Partners agree that any personal information requested or disclosed, should be restricted to the minimum amount of information necessary to achieve the purpose, and where appropriate, be as generalised as possible. Personal information should not be disclosed where de-personalised information (that is to say, the information where the individual cannot be identified) would suffice.

When sharing de-personalised information with other organisations, partners expect the information to only be used for the original purpose of the disclosure and that it will not be processed in such a way that information about a living and identifiable individual may be extracted from the data.



## 6. Information standards

The Data Protection Act 1998 (the DPA 1998) places a legal requirement on organisations to ensure that the personal data they hold is accurate and, where necessary, kept up to date. If a partner becomes aware that the information they hold is inaccurate, they must take appropriate action to verify and correct the information.

### Information quality

It is particularly important when sharing personal information, that the quality of the data is checked before it is disclosed. It may not be possible to check all records beforehand, in such cases partners agree to check a sample of records, where possible. If a partner does not know whether the information they are sharing is up to date, because they have not had contact with the person or family for a long time, this should be made clear to the person the information is being given to.

### Relevance

Before information is shared, partners must decide what the purpose of the sharing is. That is to say, what do they want to happen or need to happen? Once the partner has decided the purpose, it should determine how much information is needed to be shared. Information should only be shared if it is adequate, relevant and not excessive for the purpose of the sharing.

## Rectifying inaccuracies

There may be occasions when a person disagrees with the information recorded about them and claims that it is inaccurate or misleading. Individuals have the right under the DPA 1998 (Section 14) to have inaccurate information held about them rectified, blocked, erased or destroyed. It is recognised that it may be difficult or even impossible for partners to remove inaccurate entries or comments recorded on paper. In such cases it is good practice for partners to attach an additional sheet, highlighting the error and/or the individual's opinion that the information is inaccurate.

Partners agree that disputes about data accuracy will be taken seriously. If a complaint is made, the person responsible for data protection in that organisation should be consulted. Partners are not usually obliged to remove or alter an employee's opinion about an individual, unless that opinion has been based on inaccurate information.

If a partner discovers they have shared inaccurate information, they should correct their own records and make sure the information is also corrected by others holding it. If inaccurate or out of date information is not corrected, this will cause problems in terms of service delivery and may well cause the individual damage or distress.

## Retention and disposal of personal information

Partners acknowledge that the DPA 1998 requires that personal information shall not be held for any longer than necessary. Partners shall comply with their own record retention and safe disposal policies regarding this.

Partners agree that they must destroy (or return) personal information provided to them as soon as it is no longer required.

## 7. Keeping information secure

Partners will take all reasonable steps to adequately protect the personal information it holds or shares, from unauthorised or unlawful processing, accidental loss, destruction or damage and will endeavour to adopt the Information Security Standard ISO27001 for making data secure.

Partners should ensure that access to personal information by individuals employed by or engaged by them, should be restricted to those who need the information to do their job. It is good practice to maintain a full audit record of disclosures made by them.

**Appendix Three** provides a checklist for sharing information securely and will be adhered to where appropriate, by all partners.

### Incident reporting

It is good practice for partners to have in place a mechanism for staff and the public to report information security incidents (for example, data loss or theft) whether they are actual incidents or near misses. These incidents should be reported to the person responsible for information security or data protection within the relevant partner. If personal data is lost or stolen and contains information which has been provided by another partner, the originating partner must be told and kept informed of the outcome.

## 8. Access to personal information

Individuals have, amongst other rights, a right to access personal data relating to them held by or under control of an organisation. This right is under Section 7 of the DPA 1998 (Right of Access to Personal Data).

Partners will apply their own internal procedures for dealing with Subject Access requests. If the request refers to any personal data which originated from another organisation, the partner holding the data will contact the other organisation. The person responsible for data protection should be consulted regarding disclosure.

Partners 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 partners where appropriate.

## 9. Complaints

All complaints made in respect of disclosures will be brought to the attention of the nominated Partnership Contact Officer and Data Protection Officer of the relevant partner. The complaint will be dealt with in accordance with the partner's own complaints procedure.

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



## 10. Partnership contact officers

Several of the partners have nominated a Partnership Contact Officer who will be the main point of contact for their organisation for sharing information. Partnership Contact Officers are identified in **Appendix Four**.

Partnership Contact Officers will ensure information sharing training is made available to appropriate staff within their organisation. It is good practice to make sure that only staff who have received appropriate information sharing training, be allowed to request or share personal data. Partners recognise the benefits of keeping a record of staff who have been trained and are authorised to process information and make disclosures.

### **Disclosure to another organisation**

Personal information received from one partner should not be disclosed to another organisation, unless the originating partner agrees or disclosure is required or permitted by law.

## 11. Working practice information sharing agreements

Partners recognise the benefits of having working practice agreements where there are specific arrangements for sharing information about children and young people.

**Appendix Five** is a template agreement. Partnership Contact Officers should be contacted to help set up an agreement. The handling of personal data under these agreements should adhere to the recommendations set out in this Code of Practice.

Partners agree that the relevant Partnership Contact Officer and the nominated holder of this Code of Practice should be notified of any new working practice agreements, in relation to the sharing of personal information within the Devon Children's Trust Partnership. Where appropriate, working practice agreements will be published on the Children's Trust website.

The nominated holder of this Code of Practice is the Corporate Information Governance Manager for Devon County Council. Contact details can be found in **Appendix Four**.

## 12. Code of Practice review and changes

The nominated holder of this Code of Practice will make sure that it is reviewed on a regular basis, taking into account any new legislation or official guidance. This will be done on at least an annual basis.

Partners can ask for changes to be made to the Code of Practice at any time by submitting a request to the nominated holder who will circulate the requests to the Devon Children's Trust Partnership; co-ordinate responses and, where appropriate, seek agreement to the requested changes from the Trust.



## 13. Publication of the Code of Practice

This Code of Practice may be published by each of the partners in accordance with their obligations under the Freedom of Information Act 2000.

### Code of Practice change history

Version no and date: new at first release
Summary of change: amalgamation of the <i>Practitioners Guide</i> and the <i>Information Sharing Protocol</i> October 2007
Implementation date and new version no: v1.0 July 2010

## 14. Children's Trust Information Sharing Forum

A working group has been formed of Information Sharing Leads from partners across the Children's Trust. This group will:

- review information sharing policies and procedures
- audit information sharing practice across the Children's Trust partnership
- make sure individual agencies provide support to practitioners to promote effective information sharing.

If you have any issues, queries and incidents, they should be taken up with the appropriate line management and escalated to the Partnership Contact Officer if unresolved. Partnership Contact Officers can be found in **Appendix Four**.

## Laws enabling and governing the sharing of personal data

### 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.

**Section 12** - requirement on children's services authorities in England to establish and operate databases containing basic information about every child in England. The current database is known as ContactPoint.

### 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 ACPO/NIPD code of practice sets out obligations on people or receiving organisations police information to apply safeguards to protect the security and confidentiality of police information.

## National Health Service Act 2006

**Section 82** - in exercising their respective functions NHS bodies and local authorities must co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.

**Section 201** A disclosure of information is made in accordance with this subsection if it is made for the purposes of any criminal investigation or proceedings.

## Checklists for Sharing Information under the Data Protection Act 1998

### Sharing personal information

- Do I have consent from the person?
- Do I have a contractual duty to share information?
- Is the sharing necessary to comply with a legal obligation?
- Is the sharing necessary to protect the individual's life or protect them from serious harm?
- Is sharing in the public interest or necessary for my organisation or the other organisation to undertake its official duties?
- Do I or the other organisation I want to share the information with have a legitimate and lawful purpose for sharing the information and, in my view the sharing would not cause unwarranted prejudice to the rights and freedoms of the individual?

This checklist derives from the conditions listed in Schedule 2 of the Data Protection Act 1998.

### Sharing sensitive personal information

- Do I have explicit consent from the person?
- Does my organisation have a legal obligation in connection with employment e.g. to protect the health and safety of its staff?
- Is the sharing necessary to protect the life of the individual or someone else or to protect them from serious harm?
- Is sharing in the public interest or necessary for my organisation or the other organisation to undertake its official duties?
- Is the sharing necessary for medical purposes?
- Is the sharing in the substantial public interest
- Is the sharing for the purposes of preventing or detecting an unlawful act

This checklist derives from the conditions listed in Schedule 3 of the Data Protection Act 1998.

## Checklist for sharing information securely

### **Sending personal information by fax**

- Mark the cover sheet 'for the attention of the addressee only'.
- Information disclosed must be restricted to the minimum necessary for the purpose of the disclosure.
- Information disclosed must not identify a particular service user, if not required.
- Telephone the recipient beforehand, to ensure they know they will shortly be receiving a fax.
- Double check the fax number before sending. If possible, use pre-installed fax numbers to minimise the risk of misdialling.

### **Sending personal information by post**

- Mark post 'for the attention of the addressee only' and if possible protectively mark the information using the Government's Protective Marking Scheme, for example RESTRICTED, PROTECT or UNCLASSIFIED.
- Make sure envelopes and packages are effectively sealed and have the correct postage.
- Inform the designated recipient that the information has been sent and ask them to contact you if they do not receive it within the expected timeframe.
- Limit the amount of personal information disclosed to those details necessary for the recipient to carry out their role effectively.

## Sending personal information by email

- Do not send the personal information by email unless you know the whole of the transmission is through fully secure networks. Currently the only addresses using secure networks end in .pnn.gov.uk, .gsi.gov.uk, .gsx.gov.uk, .gsm.net and .nhs.net. An email to a .gov.uk address is **not secure**. Additionally an email from a .gov.uk address to any of the above addresses is **not** fully secure
- If you cannot use a secure e-mail account and must share the personal information electronically, for expediency, password-protect the document before you email it. Do not put the password in the same email. Send the password in a separate email or telephone the person giving them the password.

## Sharing personal information verbally

- Take care to ensure that your conversation cannot be overheard by others who do not need to know.
- Make sure you know who you are talking to over the phone and check that the individual is the right person to speak to.
- If you do not recognise the person calling, ask them for their name and their switchboard number and call them back using their organisations general number and not their direct office number, to ensure they are who they say they are.



## Partnership Contact Officers

### Careers South West

Information Governance Manager  
Tamar Business Park, Pennygillam  
Industrial Estate, Launceston PL15 7ED  
**01566 777672**  
**andy.tellam@careerssw.org**

### Devon and Cornwall Constabulary

Head of Information Management  
Devon & Cornwall Constabulary, Force HQ  
Middlemoor, Exeter EX27HQ  
**01392 452903**  
**john.ellis@devonandcornwall.pnn.police.uk**

### Devon County Council

Head of Information and Performance Analysis  
Children and Young People's Services  
Room 137, County Hall, Topsham Road  
Exeter EX2 4QG  
**01392 382034**  
**richard.stevens@devon.gov.uk**

Corporate Information Governance Manager,  
Room L10, County Hall, Topsham Road,  
Exeter EX2 4QD  
**01392 384682**  
**amber.steer-frost@devon.gov.uk**

### Devon Partnership NHS Trust

Information Governance Manager  
Wonford House Hospital,  
Dryden Road Exeter EX2 5AF  
**01392 403485**  
**emmy.lloyd@nhs.net**

### Devon Provider Services

Information Governance Manager  
Unit 1 Exeter International Office Park  
Clyst Honiton, Exeter EX5 2HL  
**01392 356918**  
**sue.smith22@nhs.net**

### NHS Devon - Commissioning

Information Governance Manager  
County Hall, Topsham Road, Exeter EX2 4QL  
**01392 205205**  
**foi.devonpct@nhs.net**

### Devon and Cornwall Probation Trust

Assistant Chief Officer - North and East Devon  
3/5 Barnfield Road, Exeter EX1 1RD  
**01392 455416**  
**charlotte.coker@devon-cornwall. probation.gsi.gov.uk**

### Devon Youth Offending Service

YOS Manager  
Ivybank, 45 St David's Hill, Exeter EX4 3LJ  
**01392 384963**  
**sue.mcgrath@devon.gov.uk**

### Northern Devon Healthcare NHS Trust

Information Governance Lead  
Suite 8, Munro House, North Devon District  
Hospital, Barnstaple EX31 4JB  
**01271 311682**  
**david.lawrence@ndevon.swest.nhs.uk**

## **Royal Devon and Exeter NHS Foundation Trust**

Information Governance Manager  
Royal Devon and Exeter Hospital  
Barrack Road, Exeter EX2 5DW  
**01392 402261**  
**sharon.collingwood@rdefn.nhs.uk**

## **South Devon Healthcare NHS Trust**

Information Governance Manager  
Hengrave House, Torbay Hospital  
Newton Road, Torquay TQ2 7AA  
**01803 654868**  
**judy.crathorne@nhs.net**

## **South Western Ambulance Services NHS Trust**

Information Governance Manager  
Westcountry House, Unit 3 Abbey Court  
Eagle Way, Sowton Industrial Estate  
Exeter EX2 7HY  
**01392 261514**  
**carla.bryan@swast.nhs.uk**

## **Voluntary Sector Organisations**

Head of Information and Performance Analysis  
Children and Young People's Services  
Room 137, County Hall, Topsham Road  
Exeter EX24QG  
**iisam@devon.gov.uk**

# Appendix Five - Template

<b>Working practice agreement for the sharing of: XXXXX</b>	
Between <b>XXXX</b>	and <b>XXXXX</b>
Version: <b>XX</b>	Date: <b>XX</b>
<p><b>Introduction</b></p> <p>This is an agreement between <b>XXXX</b> and <b>XXXX</b> for the sharing of <b>XXXXXX</b> for the purposes of <b>XXXX</b></p> <p>This agreement is supported by the Devon Children’s Trust Code of Practice for sharing Children and Young People’s Information.</p> <p>It is not intended that this document will repeat the guidance provided by the Code of Practice but will highlight specific sharing arrangements between the partners stated.</p>	
<b>1. Law governing and enabling the sharing of personal data under this agreement</b>	
Act	Section
<b>Other relevant information such as Home Office Circulars or Regulations:</b>	
<b>2. Information to be shared under this agreement by xxxxx [party one]</b>	
• <b>XXXX</b>	
• <b>XXXX</b>	
• <b>XXXX</b>	

<b>3. Action by xxxxx</b> xxxx has agreed to provide the information stated above where the law permits disclosure. xxxx will disclose this information in the following circumstances:
• xxxxx
• xxxxx
• xxxxx
<b>4. Information to be shared under this agreement by xxxxx [party two]</b>
• xxxxx
• xxxxx
• xxxxx
<b>5. Action by xxxxx</b> xxxx has agreed to provide the information stated above where the law permits disclosure. xxxx will disclose this information in the following circumstances:
• xxxxx
• xxxxx
• xxxxx
<b>6. Sharing personal information securely</b> Each partner agrees to follow their own internal policies and guidance on sharing information securely and recognises the good practice recommendations of the Devon Children's Trust: Code of Practice for sharing children and young people's information.
<b>7. Disclosure of personal data to another agency</b> Partners agree they will only use the information they are given for the original purpose of the disclosure. Partners agree not to share the information with another organisation or individual without obtaining the originating organisation's consent, unless disclosure is required or permitted by law.

# Appendix Five - Template

## 8. Indemnity clause

Partners shall indemnify all other partners 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 partners 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 partner, its servants or agents, or any of the provisions of this agreement
- any processing by the indemnifying partner, its servants or agents, of personal data received, for purposes other than the originating purpose, or
- any breach of the indemnifying partner, its servants or agents, of any law in respect of its processing of personal data received by reason of a disclosure made by another partner.

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

## 9. Partnership Contact Officers

Name and job title	Organisation	Contact details

## 10. Review of this agreement

The Nominated Holder of this agreement is xxxxx who shall, on behalf of the partners to this agreement, instigate a review of this document every 12 months.

The next review date is

## 11. Certification of this agreement

By signing below, partners accept the working practice arrangements set out in this agreement and recognise the good practice recommendations of the Devon Children's Trust: Code of Practice for sharing children and young people's information.

<b>Signed</b>	
<b>By</b>	Enter name and position of person signing
<b>For and on behalf of</b>	Insert full name of organisation

**Date:**

## Working practice agreement change history

Version no and date	Summary of change	Implementation date and new version no
xxxx	xxxx	xxxx xxxx

## Other sources of advice and guidance

Information Sharing Guidance for Practitioners and Managers

<http://publications.everychildmatters.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-00807-2008&>

Information Sharing Pocket Guide

<http://publications.everychildmatters.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-00808-2008&>

Information Sharing: Case Examples

[www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/](http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/)

Information Sharing: Further Guidance on Legal Issues

[www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/](http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/)

Information Sharing: Quick Reference Guide

<http://publications.everychildmatters.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-01070-2008&>

Information Sharing Posters

[www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/](http://www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00340/)

Department for Children, Schools and Families (DCSF): Every Child Matters

[www.dcsf.gov.uk/everychildmatters/](http://www.dcsf.gov.uk/everychildmatters/)

Information Commissioner's Office

[www.ico.gov.uk](http://www.ico.gov.uk)

Helpline **01625 545745**

ICO Privacy Notices Code of Practice

[www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/privacy\\_notices.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/privacy_notices.aspx)

The nominated holder of this Code of Practice is Amber Steer-Frost, Corporate Information Governance Manager, Devon County Council.

If you have any queries about the content or would like to request a change email [dpoffice@devon.gov.uk](mailto:dpoffice@devon.gov.uk) or telephone **01392 384682**.

For more copies of this Code of Practice email [childrens.trust@devon.gov.uk](mailto:childrens.trust@devon.gov.uk)

Find more information about the Devon Children's Trust at [www.devonchildrenstrust.org.uk](http://www.devonchildrenstrust.org.uk)



July 2010 **Version 1.0**

## **Devon Children's Trust**

email [childrens.trust@devon.gov.uk](mailto:childrens.trust@devon.gov.uk)

telephone **01392 382628**

[www.devonchildrenstrust.org.uk](http://www.devonchildrenstrust.org.uk)