
**Suffolk
Children's Trust
Partnership**

SUFFOLK CHARTER

**Information Sharing to Improve
Services for Children, Young People
and their Families**

**February 2009
Version 3**

Introduction

The aims of safe information sharing within the law are to ensure that children and young people:

- Are healthy
- Stay safe
- Enjoy and achieve
- Make a positive contribution
- Achieve economic well-being

The decision to share or not to share information about a child should always be based on professional judgement, supported by the cross-Government *Information Sharing: Practitioners' Guide* (published in April 2006) and informed by training. DCSF March 2007

The aim of this document is to improve information sharing amongst practitioners and organisations that work with children, young people and families.

This document has two parts:

The charter is a commitment by organisations to work together for the benefit of sharing information.

The protocol and appendices detail the actions that organisations will take to ensure that they share information when it is legal and necessary to do so.

Suffolk charter for sharing information for children, young people and their families

This charter is an agreement, in principle, to share information between agencies and organisations that work with children, young people and families.

The purpose of the charter is to document the information sharing protocol to be used between agencies that work with children and young people in Suffolk.

The aims of information sharing are:

- to promote the well being and safeguard the welfare of young people
- to prevent young people from being excluded and getting involved in crime
- to improve the health and well being of children and young people
- to make sure children and young people achieve their full potential

Organisations signing the charter agree:

- to share information, unless it is unlawful to share it, or consent has not been given (except where there is overriding public interest to share without consent).
- to develop good practice in the sharing of information
- to guide partner organisations on how to share personal information lawfully
- to develop Data Exchange Agreements
- to develop Data Handling Agreements
- to agree common goals in the way they share information

This charter provides a framework for secure and lawful information sharing to give children, young people and their families confidence that we use information they give us responsibly. It will also help assess and plan services for vulnerable children and young people.

Each organisation signing the charter will be responsible for:

- ensuring that the charter and protocol are put into practice

- making sure they have measures in place to protect the security and integrity of personal information
- promoting awareness and providing training for practitioners on the requirements of information sharing
- ensuring that the law and good practice are adhered to (see Appendix B)
- Sharing information between agencies, if it is lawful to do so
- having a process for obtaining consent when information is to be shared or requested (an example leaflet and consent form are contained in Appendix E)
- ensuring compliance with the Data Exchange Agreements and Data Handling Agreements in which they are involved (with responsibility allocated to a specified named person/people and reviewed annually)

Appendix E sets out the principles of Data Sharing Agreements and contains an example format for charter members to develop Information Sharing Agreements between themselves (see Appendix E). This may also be used for groups of organisations. Each agreement will contain procedures for professionals to follow when sharing information and handling shared information.

Obtaining consent is an essential step in information sharing. However there may be occasions when information can be shared without consent (see Protocol Section 8.3). Charter organisations agree that consent will always be sought except in those situations when a request may cause significant harm to an individual or prejudice the investigation of a crime or when it is in the vital interest of the child/young person to share it.

This charter and protocol does not supersede or override the Suffolk Safeguarding Children's Board Joint Policies and Procedures under "Working Together to Safeguard Children" which is still in operation and will be referred to by partner organisations when working with children at risk of abuse. For further information go to www.suffolkscb.org.uk

This charter and protocol will be reviewed annually by Suffolk Children's trust in order to further develop the practice of information sharing in Suffolk.

Suffolk Charter for Sharing Information

Inter-Agency Protocol

PROTOCOL CONTENTS

1. INTRODUCTION
2. GENERAL PRINCIPLES
3. THE LEGAL FRAMEWORK
4. CALDICOTT PRINCIPLES
5. DATA COVERED BY THIS PROTOCOL
6. PERSONAL INFORMATION
7. ANONYMISED DATA
8. PURPOSES FOR SHARING INFORMATION
9. RESTRICTIONS ON THE USE OF INFORMATION SHARED
10. CONSENT
11. ORGANISATIONAL RESPONSIBILITIES
12. INDIVIDUAL RESPONSIBILITIES
13. REVIEW ARRANGEMENTS

APPENDICES

APPENDIX A:	SIGNATURES AND CONTACT INFORMATION
APPENDIX B:	RELEVANT LEGISLATION
APPENDIX C:	CALDICOTT PRINCIPLES
APPENDIX D:	GLOSSARY OF TERMS
APPENDIX E:	DATA EXCHANGE AGREEMENT PRINCIPLES AND TEMPLATE
APPENDIX F:	MATERIALS TO SUPPORT PRACTITIONERS (weblink www.ecm.gov.uk/informationsharing) INCLUDING EXAMPLE CONSENT FORM

1. Introduction

- 1.1 This document is a Data Sharing Charter for key organisations that supply services to children and young people in Suffolk. The aim of this document is to facilitate sharing of information between the public, private and voluntary sectors so that children, young people and their families receive the services they need.
- 1.2 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal information is lawful, properly controlled and that an individual's rights are respected. This balance between the need to share information to provide quality services and protection of confidentiality is often a difficult one to achieve.
- 1.3 The legal situation regarding the protection and use of personal information is not always understood. This situation may lead to information not being available to those who have a genuine need to know in order for them to do their job properly (See Appendix B for relevant legislation).
- 1.4 Organisations working with children/young people and their families have additional responsibilities to ensure that children and young people are protected and safe from harm.
- 1.5 The information referred to in this protocol includes that gathered and held electronically or manually (e.g. information held on computer or in paper files).

2. GENERAL PRINCIPLES

- 2.1** By agreeing to the terms of the charter organisations are committed to meeting the aims stated within it. The purpose of this Protocol is to provide a legal and practical framework for charter organisations both to establish and regulate working practices to meet these aims.
- 2.2** The principles outlined in this Protocol are recommended good standards of practice or legal requirements that must be adhered to by all charter organisations.
- 2.3** This Protocol sets the core standards applicable to all charter organisations and should form the basis of all Data Exchange Agreements and their supporting Data Handling Agreements established to secure the flow of personal information.
- 2.4** This Protocol should be used in conjunction with local service level agreements, contracts or any other formal agreements that exist between the charter organisations.
- 2.5** All signatories to the Protocol are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that practitioners are properly trained to understand their responsibilities and comply with the law.
- 2.6** This Protocol has been written to set out clear and consistent principles that satisfy the requirements of the law that all practitioners must follow when using and sharing personal information.
- 2.7** The specific purposes for the use and sharing of information will be defined in the Data Exchange Agreements that will be specific to the charter organisations sharing information.
- 2.8** The operational and technical detail of how the shared information will be managed (i.e. received/dispatched, recorded, stored, processed and disposed of) during its lifetime will be defined in the Data Handling Agreements that underpin the Data Exchange Agreements.

3. THE LEGAL FRAMEWORK

- 3.1** The principal legislation and common law concerning the protection and use of personal information is listed below and further explained in Appendix B:
 - Data Protection Act 1998
 - Human Rights Act 1998 (article 8)
 - Freedom of Information Act 2000
 - The common law duty of confidence

- Children Act 1989
- Crime and Disorder Act 1998
- Children Act 2004

4. THE CALDICOTT PRINCIPLES

- 4.1** The Caldicott principles (see appendix C) govern the exchange of patient-identifiable information. They apply to all NHS organisations and are relevant to the exchange of information between the NHS and other bodies. The principles can be used by all practitioners working for charter organisations as “good practice” when considering whether to share/request information. They have been included in “Guidance for practitioners when sharing information” (see appendix F).
- 4.2** All signatories to the Protocol recognise the responsibility that Caldicott places on Health organisations in sharing information relating to children/young people.

5. DATA COVERED BY THIS PROTOCOL

- 5.1** All personal and anonymised information as defined in the Data Protection Act 1998 (DPA).

6. PERSONAL INFORMATION

- 6.1** The term ‘personal information’ refers to **any** information held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that information.
- 6.2** The term is further defined in the DPA as data relating to a living individual who can be identified:
from those data, or
from any other information which is in the possession of, or is likely to come into the possession of the data controller (the person or organisation collecting that information).
- 6.3** The DPA also defines certain classes of personal information as ‘sensitive data’ where additional conditions must be met for that information to be used and disclosed lawfully. For example, sensitive data may include: racial origin, political opinions, medical records, and religious beliefs.
- 6.4** An individual may consider certain information about themselves to be particularly ‘sensitive’ and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

- 6.5 In general, people have a right to choose how their data is used and who may have access to it. However the safety and direct interest of the child can over-ride this right. There are also other 'exceptions' set out in the Data Protection Act 1989.

7. ANONYMISED DATA

- 7.1 Charter organisations must ensure that anonymised data, especially when combined with other information from different agencies, **does not** identify a child/young person, either directly or by summation.
- 7.2 Anonymised data about a child/young person can be shared without consent in a form where the identity of the child/young person cannot be recognised i.e. when:
reference to any data item that could lead to a child/young person being identified has been removed;
the data cannot be combined with any data sources held by a partner organisation to produce personal identifiable data.
Examples of when anonymised data can be used include for research purposes and as part of evaluation of services can be found at <http://www.dh.gov.uk/Home>
- 7.3 Anonymising data does not remove the duty of confidence.

8. Purposes for Sharing Information

- 8.1. Information should only be shared for a specific lawful purpose or where appropriate consent has been obtained.
- 8.2. Practitioners should only have access to personal information on a justifiable **need to know** basis in order for them to perform their duties in connection with the services they are there to deliver.
- 8.3. Having this agreement in place does not give license for unrestricted access to information held by another charter organisation. It establishes the parameters for the safe and secure sharing of information for a justifiable **need to know** purpose.
- 8.4. Every practitioner has an obligation to protect confidentiality and a duty to disclose information only to those who have a need to see it.
- 8.5. All practitioners will be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information.**
- 8.6. All practitioners and their support staff will follow the principles and standards that have been agreed and incorporated within this

Information Sharing Protocol and any associated Data Exchange Agreements and Data Handling Agreements.

8.7. Each charter organisation will operate lawfully in accordance with the 8 Data Protection Principles (see Appendix B section1).

8.8. Personal data shall not be transferred to a country or territory outside the European Economic Area (See appendix B; subsection 1) without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

9. RESTRICTIONS ON THE USE OF INFORMATION SHARED

9.1 Information exchanged between partner organisations must only be used for the purpose(s) specified at the time of disclosure(s) (or as defined in the relevant Data Exchange Agreement). It is a condition of access that it must not be used for any other purpose without the permission of the partner organisation that supplied the data, unless an exemption applies within the Data Protection Act 1998.

10. CONSENT

10.1 Consent has to be documented by some communication between the organisation and the child/young person/carer (See appendix F for guidance on obtaining consent). If the data subject does not respond this cannot be assumed as implied consent.

10.2 If consent is used as a basis for disclosure, the child/young person/carer must have the right to withdraw consent at any time. When using sensitive personal data, explicit consent must be obtained. In such cases the child/young person/carer's consent must be clear and cover issues such as the specific details of processing, the data to be processed and the purpose for processing. It may sometimes be lawful to share information without consent (see S.10.5 below).

10.3 When obtaining consent from children, young people and their families, charter organisations will seek to obtain consent from all parties. However if a child or young person is under the age of 18 and demonstrates a sufficient level of maturity and is informed enough to make their own decision (either against the wishes of the parent/carer or if the parent/carer is not present to consent), it is possible to comply with the young person's wishes. This is sometimes referred to as "Fraser" or "Gillick" competence. Each case will have to be dealt with on an individual basis, the issue under consideration being "does the young person understand the nature and consequences of information being exchanged between agencies?"

10.4 The consent given must be "informed" i.e. the child/young person/carer must be made aware of what information is to be shared, who it is to be shared with and what it is to be used for. In addition they must have the

capacity to be able to give consent i.e. they have capacity to understand, weigh and retain the information relevant to the decision and the consequences of giving consent.

- 10.5 Consent is not the only means by which data can be disclosed. Under the Data Protection Act 1998 in order to disclose personal information without consent at least one condition in Schedule 2 must be met. In order to disclose sensitive personal information without consent at least one condition in schedule 2 and one condition in Schedule 3 of the DPA must be met (see appendix B – the schedules are not to be confused with the 8 data protection principles).
- 10.6 Where a charter organisation has a statutory obligation to disclose personal information then the consent of the child/young person or carer is not required; but the practitioner should inform the child/young person or carer about their statutory obligation.
- 10.7** The circumstances where it may be appropriate to disclose sensitive personal information can include the following terms:
- where a child is believed to be at risk of harm (Children Act 1989)
 - where there is evidence of serious risk to an individual (Data Protection Act 1998)
 - where there is evidence of a serious health risk to an individual (Data Protection Act 1998)
 - for the prevention and detection of crime (Data Protection Act 1998)
 - where instructed by a court to do so (Data Protection Act 1998)
 - for a medical emergency (Data Protection Act 1998)
 - when legally required
- 10.8 If a charter organisation decides not to disclose some or all of any personal information that has been requested, the requesting authority must be informed.
- 10.9 Because of the complexity of this area and the potential risk for agencies, decisions to share personal/sensitive information without consent will only be taken by staff with an appropriate level of authority, unless the risk to the child/young person is so serious that immediate action is required. Practitioners should follow their own agency safeguarding protocols and refer to Suffolk Safeguarding Children Board's procedures.
- 10.10 Charter organisations are responsible for ensuring that practitioners or managers taking on this role are provided with clear guidance to enable them to decide whether there are statutory grounds for disclosure without consent and should have access to appropriate legal advice provided by the partner organisation.

11. ORGANISATIONAL RESPONSIBILITIES

- 11.1 Each charter organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Protocol.
- 11.2 Charter organisations will agree the information classification and the security levels needed on supplied information and handle the information accordingly.
- 11.3 Charter organisations accept responsibility for independently or jointly auditing compliance with the Data Exchange Agreements and Data Handling Agreements in which they are involved. This role will be allocated to a specified named person/people and will take place on an annual basis.
- 11.4 Every charter organisation will make it a condition of employment that practitioners will abide by their rules and policies in relation to the protection and use of confidential information. This condition will be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation's disciplinary procedures.
- 11.5 Every charter organisation will ensure that their contracts with external service providers abide by their rules and policies in relation to the protection and use of confidential information.
- 11.6 The charter organisation originally supplying the information will be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.
- 11.7 Charter organisations will have documented policies for retention, weeding and secure destruction of personal data.
- 11.8 Charter organisations will have documented policies for how their data quality is assured and/or checked prior to sharing.
- 11.9 Charter organisations will have a documented process for receiving and managing complaints relating to any aspect of information management and sharing.
- 11.10 Every charter organization will ensure their practitioners and their support staff are trained and are fully aware of their responsibilities to maintain the security and confidentiality of personal information.

12. INDIVIDUAL RESPONSIBILITIES

- 12.1 Every practitioner working for the charter organisations is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

- 12.2** Every practitioner should know how to obtain, use and share information they legitimately need to do their job.
- 12.3** Every practitioner has an obligation to request proof of identity and to take steps to validate the authorisation of another before disclosing any information.
- 12.4** Every practitioner should uphold the general principles of confidentiality follow the rules laid down in both in this Protocol and their own organisation's procedures and seek advice when necessary.
- 12.5** Every practitioner should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal.

13. REVIEW ARRANGEMENTS

- 11.1** This overarching agreement will be formally reviewed annually unless legislation or government guidance necessitates an earlier review.
- 11.2** Any of the signatories to the Protocol can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.

Appendix A- Signatures and contact information

Suffolk Children's Trust Board

Name	Title	Organisation
Allison Coleman	Chair	Suffolk Governors Forum
Mike Stonard	Chief Executive Officer	Great Yarmouth and Waveney Primary CareTrust
Tracy Dowling	Director for Strategic Commissioning	Suffolk PCT
John Babraff	Board Chair	Suffolk Probation Service
Dawn Henry	Chief Executive	Young Suffolk
Doreen Savage	Councillor	Suffolk Coastal District Council
Steve Allman	Chief Executive - Out and About	Young Suffolk
Nadia Cenci	Councillor	Ipswich Borough Council
Patricia O'Brien	County Councillor	Suffolk County Council
Peter Worobec	Independent Chair of Safeguarding Children Board	
Rebecca Hopfensperger	County Councillor	SCC
Sue Thomas	County Councillor	Suffolk Police Authority
Johanna Finn	Independent Consultant	Learning & Skills Council

Suffolk Children's Trust Executive Group

Name	Title	Organisation
Jacqui Cheer	Deputy Chief Constable	Suffolk Constabulary
Vacancy		Great Yarmouth and Waveney Primary Care Trust
Arthur Charvonia	Asst Chief Executive	Waveney District Council
Bud Simpkin	Chief Executive Officer	Young Suffolk
Carole Herries	Head of Environmental Health and Housing	St Edmundsbury Borough Council
Sharon Singleton	Head of Children and Young People's Commissioning)	Gt Yarmouth/Waveney Suffolk PCT and SCC
Chris Fry	Portfolio Director	Mid Suffolk District Council
Jonathan Owen	Director	Ipswich Borough Council
John Budd	Chief Probation Officer	Suffolk Probation
Judith Mobbs	Area Director	Learning & Skills Council
John Gregg	Strategic Commissioner	Suffolk County Council
Odran Doran	Headteacher	Heathside School
Peter Bradley	Director of Public Health & Health Improvement	Suffolk PCT
Rosalind Turner	Director for Children & Young People	Suffolk County Council
Simon Phelan	Head of Community Development	Forest Heath District Council
Tim Mutum	Head of Leisure & Community Services	Babergh District Council
Tony Osanski	Strategic Director	Suffolk Coastal District Council

Appendix B: Relevant Legislation

1. **The Data Protection Act 1998** governs the protection and use of **personal** data. The Act does not apply to personal data relating to the deceased.

Any organisation processing (obtaining, holding, using, disclosing and disposing) data is a 'Data Controller' responsible for abiding by the 8 data protection principles and notifying the Information Commissioner of that processing.

The Act gives seven rights to individuals in respect of their own personal data:

- right of subject access
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- rights in relation to automated decision taking
- the right to take action for compensation if the individual suffers damage or damage and distress (as a result of any breach of the Act)
- the right to take action to rectify, block, erase or destroy inaccurate data
- the right to request the Information Commissioner to make an assessment as to whether any provision of the Act has been contravened

The Data Protection Act 1998 – 8 Principles

The key principles of the Act are:

1st Principle - Personal data shall be processed fairly and lawfully and shall not be processed unless at least 1 of the conditions in Schedule 2 are met and for 'sensitive personal data' at least 1 of the conditions in Schedule 3 are also met.

2nd Principle - Personal data shall be obtained for specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose/purposes.

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

4th Principle - Personal Data shall be accurate and, where necessary, kept up to date

5th Principle - Personal data shall not be kept for longer than is necessary for that purpose/purposes.

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

7th Principle - Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

8th Principle - Personal data shall not be transferred to a country or territory outside the EEA (this includes Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom, Iceland, Norway and Liechtenstein) without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Schedule 2 and Schedule 3 conditions:

The condition for processing personal data is that one condition in Schedule 2 should be met.

The condition for processing sensitive personal data is one condition in Schedule 2 and a condition in Schedule 3 should also be met.

Schedule 2: Personal Data

The data subject has given consent, or the processing is necessary:

- to establish or perform a contract with the data subject
- to comply with a legal obligation
- to protect the vital interests of the data subject or another person
- for the administration of justice, to exercise a statutory function, to exercise other functions of the Crown, a minister or a government department or to exercise any other public function in the public interest
- for the legitimate interests of the data controller unless outweighed by the interests of the data subject

Schedule 3: Sensitive Personal Data

The data subject has given explicit consent or:

- where the processing is necessary for the administration of justice, to exercise a statutory function, or to exercise other functions of the Crown, a minister or a government department;
- to perform any right or obligation of the data controller under employment law
- in connection with legal proceedings, obtaining legal advice or defending legal rights
- to protect the vital interests of the data subject (where consent cannot be obtained)
- where the data has been made public by the data subject
- for the prevention or detection of an unlawful act
- for the legitimate interests of a nonprofit making organisation
- for medical purposes

Section 29 of The DPA permits disclosure of personal information without consent for the purposes of the prevention or detection of crime, and the apprehension or prosecution of offenders where these purposes would be likely to be prejudiced by non-disclosure. The information should only be provided to the police if the request is made using a section 29(3) form.

The disclosure of personal information without consent must be justifiable on statutory grounds. It must meet one of the conditions of schedule 2 of the DPA. In addition, the disclosure of sensitive information without consent must meet one of the conditions of schedule 3 of the DPA.

2. The Human Rights Act 1998

The Human Rights Act 1998 incorporates into our domestic law certain articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law to be read in conjunction with the Convention.

It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a Public Authority fail to do so it may be the subject of a legal action under section 7. This is an obligation not to violate human rights, and a positive obligation to uphold these rights. The sharing of information between agencies has the potential to infringe a number of Convention rights in particular a right to respect for private and family life.

Article 8.1 provides that “everyone has the right to respect for his private and family life, his home and his correspondence”.

Article 8.2 provides “there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country for the prevention of crime and disorder, for the protection of health and morals or for the protection of the rights and freedoms of others”.

There is a qualification to Article 8 that “there shall be no interference by a public authority with this right unless it is in the interests of national security, public safety, the economic well being of the country, the prevention of disorder and crime, the protection of health and morals, or the protection of the rights and freedoms of others”. In addition, all Convention rights must be secured without discrimination on a wide variety of grounds under article 14. The Convention does allow interference with the Convention rights by public authorities under certain broadly defined circumstances known as legitimate aims. However, mere reliance on a legal power may not alone provide sufficient justification and the following principles should be considered:

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

3. The Freedom of Information Act (FOIA) 2000

The Freedom of Information Act 2000 applies to all public authorities. The Act creates new rights of access to information (rights of access to personal

information will remain under the Data Protection Act) and revises and strengthens the Public Records Act 1958 & 1967 by re-enforcing records management standards of practice.

The Lord Chancellor has issued a code of practice on the management of records under the FOIA. The principle is that *“any freedom of information legislation is only as good as the quality of the records to which it provides access. Such rights are of little use if reliable records are not created in the first place”*. Further information guidance can be found at the following web site <http://www.informationcommissioner.gov.uk/>

4. The Common Law Duty of Confidentiality

The common law duty of confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest i.e. to protect others from harm.

5. The Children Act 1989

Section 27 allows for local authorities that provide services to children and families under the Act to request help from any local authority, any local housing authority, any local education authority and any health authority or NHS Trust provided that help is compatible with the other authorities' duties and functions. This would cover disclosure of personal data necessary to enable assistance to be given to protect children from harm. Section 47 places a duty on these authorities to comply with the request provided that the request is not incompatible with the performance of its own obligations and would not unduly prejudice the performance of its own functions.

6. The Crime and Disorder Act 1998

Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities where disclosure is necessary or expedient for the purposes of any provision of the Act and where they do not already have the power to do so. However whilst agencies have the power to disclose section 115 does not impose a requirement on them to exchange information and responsibility for the disclosure remains with the agency holding the information.

7. The Children Act 2004

Section 10 of the Act requires local authorities and other key bodies to make arrangements to cooperate with a view to improving the well-being of children in the authority's area with regard to –

- physical and mental health and emotional well-being;

- protection from harm and neglect;
- education, training and recreation;
- the contribution made by them to society;
- social and economic well-being.

Section 11 of the Act places a duty on children's services authorities; district councils; strategic health authorities; special health authorities; primary care trusts; NHS trusts; NHS foundation trusts; police authorities; chief officers of police; probation boards; youth offending teams; governors/directors of prisons or secure training centres; and any person providing services under section 114 of the Learning and Skills Act 2000 to make arrangements to ensure that their functions are discharged having regard to the need to safeguard and promote the welfare of children.

It is a necessary part of the fulfilling of these duties that information about children and their families is shared appropriately.

Section 12 of the Act creates a power for the Secretary of State, by regulations, to require local authorities to establish and operate a database or databases of information about all children and other young people to whom arrangements under section 10 or 11 or section 175 of the Education Act 2002 may relate. The Information Sharing Index (England) Regulations 2006 were passed onto the statute books on 1st August 2007. The index is known as ContactPoint and is expected to be rolled out nationally from early 2009.

Appendix C – Caldicott Principles

The Caldicott Committee (1997) carried out a review of the use of patient identifiable information. It recommended a series of principles that should be applied when considering whether confidential patient-related information should be shared. All NHS organisations and Social Services Departments are now required to apply the Caldicott principles.

1st Principle - Justify the purposes

Every proposed use or transfer of 'patient or client-identifiable information' (where the individual can be identified) within or from an organisation should be clearly defined and inspected. Continuing use should be regularly reviewed by an appropriate person (known as the Caldicott Guardian).

2nd Principle - Don't use patient or client-identifiable information unless it is absolutely necessary

Patient or client-identifiable information should not be used unless there is no alternative.

3rd Principle - Use the minimum necessary patient or client-identifiable information

If using patient or client-identifiable information is essential, each individual item of information should be justified with the aim of reducing the possibility of an individual being identified.

4th Principle - Access to patient or client-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient or client-identifiable information should have access to it, and they should only have access to the information they need to see.

5th Principle - Everyone should be aware of their responsibilities

Action should be taken to make sure that those handling patient or client-identifiable information (clinical, non-clinical and non-health staff) are aware of their responsibilities to respect confidentiality of patients and clients.

6th Principle - Understand and follow the law

Every use of patient or client-identifiable information must be legal. Someone in each organisation should be responsible for making sure that the organisation meets legal requirements.

Appendix D: Glossary of Terms

Accessible Record	any recorded personal information usually but not always in manual form relating to health, education, social work and housing
Agent	acts on behalf of the data subject
Aggregated	collated information in a tabular format e.g. statistical data
Anonymous data	anonymous data is where an organisation does not have the means to identify an individual from the data they hold. If the data controller has information which allows the data subject to be identified, regardless of whether or not they intend to identify the individual, this is not anonymous data. The data controller must be able to justify why and how the data is no longer personal.
CCTV	closed circuit television
Consent	to give permission or approval for something to happen

The Information Commissioner's legal guidance to the Data Protection Act 1998 is to refer to the EU Directive, which defines consent as "...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed"

Data	a) Information being processed by means of equipment operating automatically; or b) Information recorded in order to be processed by equipment; or c) Information recorded as part of a relevant filing system; or d) Information not in a or b or c, but forming part of an accessible record
Data Controller	a person or a legal entity such as a business or public authority who jointly or alone determines the purposes for which personal data is processed
Data Exchange Agreement	the local information sharing agreement based on the attached template Appendix E
Data Flows	the movement of information internally and externally, both within and between organisations
Data Processing	any operation performed on data. The main examples are collection, retention, deletion, use and disclosure
Data Processor	operates on behalf of the data controller
Data Set	a defined group of information
Data Subject	an individual who is the subject of personal information
Disclosure	the passing of information from the data controller to another organisation/individual

Duty of Confidentiality	everyone has a duty under common law to safeguard confidential information
European Economic Area (EEA)	this consists of the twenty five European Union members together with Iceland, Liechtenstein and Norway
Fair processing	to inform the data subject how the data is to be processed before processing occurs
Health Practitioner	In the Data Protection Act 1998 "health practitioner" means anyone of the following who is registered as: A medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or health visitor, and osteopaths. Also any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 currently extends: clinical psychologists, child psychotherapists and speech therapists, music therapists employed by a health service body, and scientists employed by such a body as head of department
Health Record	any information relating to health, produced by a health practitioner
Need to know	to access and supply the minimum amount of information required for the defined purpose
Personal Data	means data relating to a living individual who can be identified from that data (including opinion and expression of intention)
Processing	any operation performed on data. Main examples are to collect, retain, use, disclose and delete
Purpose	the use / reason for which information is stored or processed
Recipient	anyone who receives personal information except statutory bodies for the purpose of specific inquiries
Relevant Filing System	two levels of structure, (i) filing system structured by some criteria (ii) each file structured so that particular information is readily accessible
Sensitive Personal Data	data concerning racial origin, political opinions, trade union activity, health, sexuality, offending, religion
Serious Crime	there is no absolute definition of "serious" crime, but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrestable offences". These include: <ul style="list-style-type: none"> ▪ Treason ▪ Murder ▪ Manslaughter ▪ Rape ▪ Kidnapping ▪ Certain sexual offences ▪ Causing an explosion

- Certain firearms offences
- Taking of hostages
- Hijacking
- Causing death by reckless driving
- Offences under prevention of terrorism legislation (disclosures now covered by the Prevention of Terrorism Act 1989)

Subject Access

the individual's right to obtain a copy of information held about them

Third Party

any person who is not the data subject, the data controller, the data processor (includes Health, Housing, Education, Carers, Voluntary Sector etc. as well as members of the public).

Appendix E: Data Sharing Agreement Principles

The Suffolk Charter document sets the strategic framework within which Suffolk County Council will share personal information both between practitioners and professionals on a case by case basis and electronically via bulk data extracts that are shared within the organisation or with external partner organisations (whether supplying or receiving them).

The layout and presentation of these agreements will be subject to any organisational standards for such documents but their minimum content is outlined below.

Data Supply Agreements

Data Supply Agreements are primarily about agreeing and establishing processes, roles and responsibilities, and are particularly relevant to the supply of bulk data extracts by electronic means from one organisation to another or within an organisation.

There should be a separate data supply agreement that covers each distinct set of data supplied between organisations. The purpose is to create a formal agreement based on the Information Sharing Protocol framework defined in the Suffolk Charter that both parties can sign up to in order to share a specific set of personal information, whether between two organisational units or partner organisations. Such an agreement should encompass:

- the legal basis for sharing (referring to any relevant legislation and DPA 1998 Schedule 2 conditions for personal information and Schedule 3 conditions for sensitive information),
- who is involved in the information sharing,
- what information is being shared (business and technical description) down to field level,
- who holds the Data Controller role within each organisation,
- how information quality for the shared data will be assured or checked,
- format and frequency of information sharing,
- how information security and confidentiality will be addressed,
- how data subjects will be advised of this use of their data (e.g. Fair Processing Notices)
- how consent (and refusal of consent) will be handled where relevant,
- how complaints will be handled

Data Handling Agreements

The data supply agreement should be underpinned by a data handling agreement. Its purpose is to document the more detailed operational and technical aspects of how shared data will be received/dispatched, recorded and managed during its lifecycle within the organisations. It should also address the classification of information. Such an agreement should encompass as a minimum:

- Receipt/dispatch of data (who, what, when, where)
- Type of data and classification (e.g. protected personal data)
- Format of data (content and structure)
- Delivery mechanisms and media
- Recording of data audit trail (see Data Register)
- Storage
- Security (including encryption)
- Backup procedures and business continuity plan
- How obsolete data/media will be destroyed

Data Register

The purpose of a Data register is to maintain a log of all shared data that is received by or dispatched from the organisation and provide an audit trail of its lifecycle within the recording organisation for security and audit purposes. It should record as a minimum:

- Organisation Name, Address, Contact Telephone Number, e-mail that the data is either sent to or received from
- Date the data was received/dispatched
- Data type and classification
- How data was transferred (delivery mechanism and media)
- How, by whom and when delivery/receipt is acknowledged
- Storage method and location
- Who has access to the data
- Purpose of use
- Date results were returned
- Date the data was returned or destroyed

Data Exchange Agreement Template (For use by organisations that want to share information)

1. Purpose of this data exchange agreement

A clear statement of why there is a need to share information between the organisations party to the Suffolk Information Sharing Charter Data Exchange Agreement (DEA), together with any relevant legislation or central government circulars that enable lawful data sharing.

For Example:

- The purpose of this Data Exchange Agreement is to co-ordinate the continued care of children between the charter organisations
- This data sharing is done under the legal framework contained in the Children's Act 1998

2. Extent and type of information to be shared

2.1 Extent of the data to be shared

The data exchanged should be the minimum amount necessary. The agreement should clearly state what information is shared routinely. You should expressly state what information you are exchanging under this agreement.

For example:

The information exchanged routinely is Client Name, Address, and Date of Birth.

7.2 Type of information to be shared

For example:

Anonymised information

Wherever possible data should be anonymised. If large volumes of data are provided for research and/or planning by charter organisations, as a matter of courtesy the outcome of that research/planning should be provided to the organisation(s) supplying the data.

3. How the information may be used

A clear statement of:

- What information is collected
- How it will be used and stored
- With whom it will/may be shared

4. Appropriate Security Levels

4.1 Each charter organisation should ensure that the information classification for the information being shared is agreed and that the minimum standards of security that they require for that classification level are in place with charter organisations that they intend sharing information with, for example:

- Storage
- How data will be transferred
- Secure destruction
- Accessibility
- Integrity
- Availability

5. Breach of Confidentiality

5.1 Items to be considered – how are you going to deal with:

- Any breach of agreement
- Internal discipline
- Monitoring security incidents
- Any malfunctions

6. Indemnity

The following text is an example that may be included:

“Recipients of information disclosed under this agreement will fully indemnify the agency sharing information against all direct and indirect losses, damages, costs, expenses, liabilities, claims or proceedings, whether these

arise under statute or common law, (together referred to as 'the losses') which it suffers as a result of any negligence, default or breach of statutory duty on the part of the receiving agency in processing the information disclosed in accordance with this agreement or on the part of any person it employs or engages to carry out its obligations in relation to the information released to it"

7. Subject Access Request

- How you will deal with Subject Access Requests
- How you will deal with any data correction request arising from a Subject Access Request
- Procedures for obtaining 3rd party consent

8. Release of 3rd Party Information

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 unless an exemption applies.

9. General Operational Guidance

9.1 Review and Weeding

Agreement should be reached between the parties as to an acceptable time period for the data to be exchanged.

An agreement of the time scales for the retention of electronic and paper based information and how the information should be securely disposed of is required.

9.2 Resource Implications

Consideration should be given to the staff time and resource implications that are involved for the Data Controller extracting the data. If a request is made and then the data is no longer required there should be a process for rescinding the request.

9.3 Appropriate Signatories

- Named individual to lead on DEA
- Who will champion training in the DEA
- Who will monitor the operation of the DEA

9.4 Data Quality

- How is the quality of the data being shared checked or assured?

9.5 Complaints

- How will any complaints in respect of data sharing, processing or handling be dealt with?

9.6 Review of Data Exchange Agreement

- How long will the DEA last
- When will the DEA be reviewed (insert date) and who will review it.

9.7 Compliance with the DEA

How are you going to ensure compliance with the DEA?

10. Closure/termination of agreement

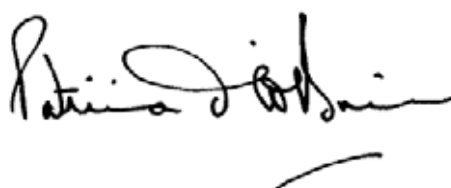
- Under what circumstance should the agreement close or terminate
- What will happen if there is a serious breach of confidentiality
- Termination/notice penalty

Any charter organisation can suspend the Data Sharing Agreement for 30 days if they feel that Security has been seriously breached. Termination and/or completion that must be given in writing with at least 30 days notice.

11. Signatories

This agreement is signed on behalf of the Suffolk Children's Trust as follows:

Name: Patricia O'Brien
Title: County Councillor
Date: 29/1/2009

Signed: 

Appendix F- Examples to assist practitioners

The decision to share or not to share information about a child should always be based on professional judgment, supported by the HM Government Information Sharing Guidance (published October 2009) and informed by training. The lack of an information sharing agreement between agencies should never be a reason for not sharing information that could help a practitioner deliver services to a child.

www.ecm.gov.uk/informationsharing

Partner organizations may have developed their own guidance for practitioners and children/young people/families it is not the intention to replace these. However if partner organisations do not have them then this guidance can be used or adapted for information sharing purposes.

Also see: Page 30 Sample Consent Form

AGREEMENT TO SHARE YOUR INFORMATION

The person working with you/your child will give you a leaflet explaining what information is held on you/your child, why it is held, why it is shared with other agencies and details about the law and your rights.

Name of Child/Young Person..... D.O.B.....

I understand that information is held about me/my child. I have had the opportunity to discuss what this means.

(Please tick ONE of the following)

- I agree that personal information about me may be shared with other agencies and with other professionals
- I agree that personal information about my child may be shared with other agencies and with other professionals
- I agree that personal information about me may be shared with other professionals, except as follows:
- I agree that personal information about my child may be shared with other professionals, except as follows:

Signature of parent/carer _____ Date _____

Signature of child/young person _____ Date _____

Signature of professional _____ Date _____

Organisation/Agency: _____

This agreement will be reviewed on/when _____

A copy must be given to the person signing the form, and an additional copy placed on the child or young person's records.