Code of practice for Information Sharing

Brighton & Hove Children and Young People's Trust

NHS

Brighton & Hove Children and Young People's TRUST

Brighton & Hove City Council

Contents

First Edition: September 2009

"It is important for professionals to trust their feelings when they perceive children to be suffering, and not make assumptions that others have also perceived it and are better placed to act. It is simpler to lift the telephone than to live with the regret of not having done so."

Serious Case Review: Baby Peter
Executive Summary
LSCB Haringey
February 2009
Paragraph 4.3.6

Preface

Our commitment to good practice Information Sharing

Brighton and Hove Children and Young People's Trust, hereafter referred to in this document as the CYPT, is a local strategic arrangement of service commissioners and providers working to a common purpose. Though united by that purpose, the trust is essentially comprised of different legal organisations, and exchange of personal information within those organisations and between those organisations needs to comply with the law.

This framework, which draws upon the guidance issued by the DCSF, NHS and the Information Commissioner's Office, will show practitioners and managers what needs to be in place, specify what is already in place, and help them understand when they may need to act, and what they may need to do.

This framework is written primarily to help workers of the CYPT and elected members understand our responsibility for legal and good practice information sharing. It is a public document and can be used to help professional partners who are not managed within the CYPT understand how their own practice can comply.

The Data Protection Act is not a barrier to sharing, rather a framework to ensure that personal information is shared appropriately and managed carefully. Brighton and Hove Children and Young People's Trust needs all staff to understand the delicate balance between preserving confidentiality and the imperative to share when this will help a child or young person achieve the five Every Child Matters outcomes. In the wake of Lord Laming's recent report, it is still true to say that no major enquiry has ever criticised staff for sharing information, rather highlighting how failures to share have contributed to childcare tragedies.

The text that follows makes explicit the CYPT code of practice. Whether practitioners or managers are employed by the council or the health trust, they can be sure that, in following the guidelines herein, they are meeting the requirements of their employing organisation, their professional codes of conduct, the DCSF, the NHS and the Information Commissioner's Office.

To help practitioners and managers share information appropriately, the CYPT has a range of materials available. Some are national publications and others locally produced. All are listed in the Appendices. We have included a sample information sharing procedure that teams can use as a template to underpin their regular processes.

South Downs Health staff working for the CYPT are still required to adhere to the NHS Code Of Conduct for Confidentiality and the NHS Code of Practice for Records Management. Though the CYPT Code of Practice aims to be congruent with these documents there are within them specific requirements for health staff. Links to those documents are listed in Appendix 4.

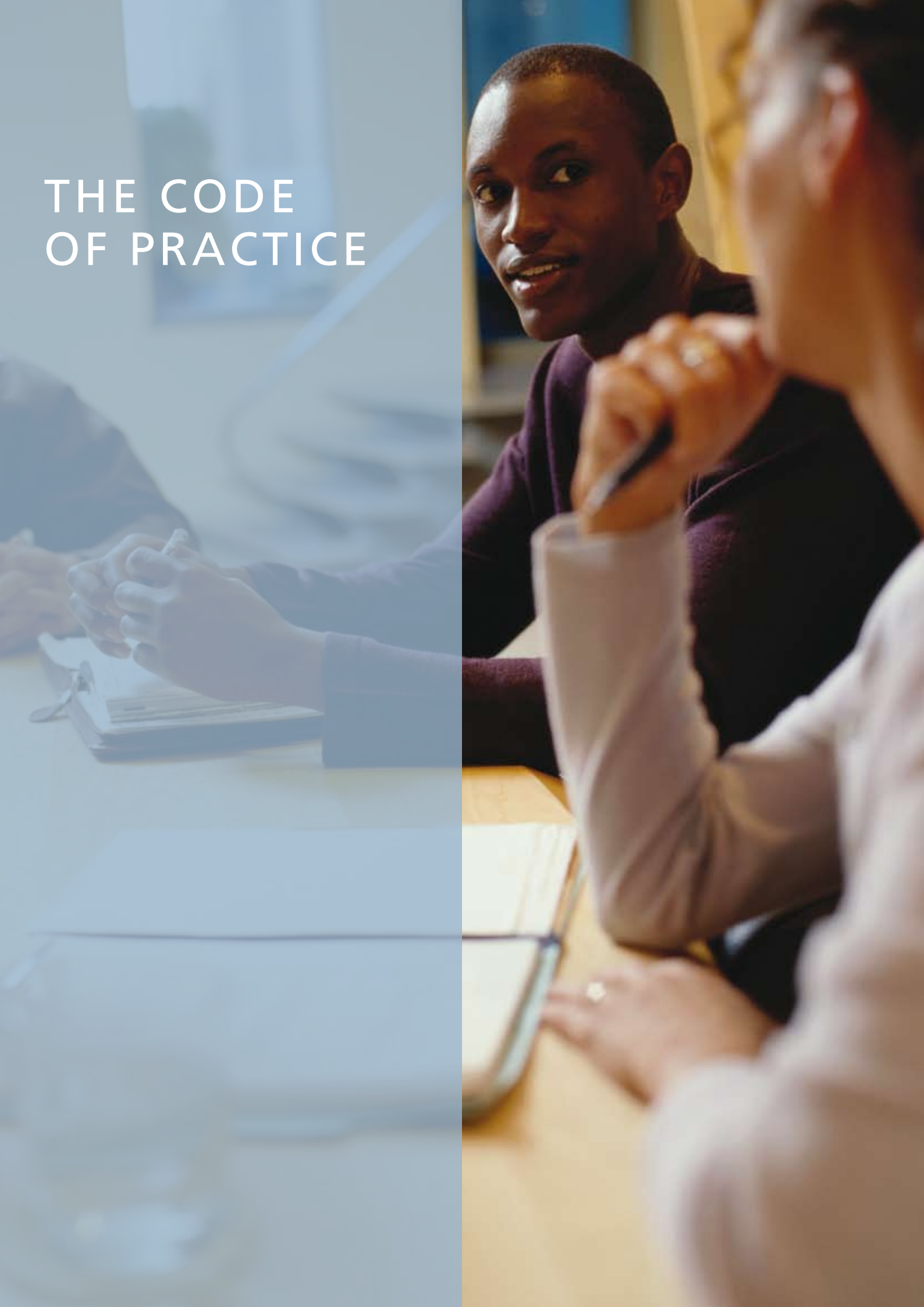
Introduction

This Code of Practice is a welcome addition to the documents and processes we are putting in place to make our Children and Young People's Trust an efficient and effective organisation that will improve the lives of our children, young people and families.

At the heart of it is the understanding that, in Brighton and Hove Children and Young People's Trust, we work as one team to meet the needs of our children. This means that information held by one member of staff employed by the CYPT about a child can, and should, be shared with colleagues in the interest of meeting the needs of that child. Of course, there will always be subtleties, complexities and exceptions. This code of practice has been produced to help us manage a best practice way through those challenges.

Di Smith
Director of Children's Services

THE CODE OF PRACTICE



1. Deciding to share personal information

The law says:

Any information sharing **must** be necessary. Any information shared must be **relevant** and **not excessive**.

The implications for organisations and individual practitioners are slightly different so they are dealt with separately below.

1. Organisations

Public sector organisations are bound by the European Convention on Human Rights. Any information sharing the CYPT carries out must be compatible with the convention, in particular the right to respect for private and family life.

The Information Commissioner's Office requires all public bodies to notify how they will process information. This means that the Brighton and Hove City Council and the South Downs Health Trust have to be explicit about the types of data processing they undertake in an annual notification to the ICO. Each organisation is required to submit its own notification and it applies to sharing information with each other as well as with outside organisations. Two examples of the types of information we may share in the CYPT are: bulk information that will inform performance management, resource deployment and service design; relevant personal information about individuals to enable effective service delivery by a limited group of practitioners working in close partnership with that individual.

Working to refine our use of data will be an ongoing process that will facilitate rather than impede the development of integrated working.

Guidelines for good practice by organisations

1 Before sharing information the organisation will need to decide the objective that it is meant to achieve, and document it. This will help resolve subsequent issues.

It is never justified to share information that identifies people when anonymised or statistical information could be used as an alternative. For example, it may only be necessary to use general demographic information about people living in certain areas, rather than identifiable individuals' names, addresses and dates of birth.

2 The organisation will need to determine at the beginning of any project who will be responsible for dealing with the various compliance issues that will arise. Where more than one organisation is involved, all the organisations involved will have some responsibility. However, the organisation that originally collected the information has the primary responsibility for making sure it is handled properly. In particular, that organisation must make sure that sharing its information will not cause real unfairness or unwarranted detriment to individuals.

3 One way of assuring good practice is to carry out a 'privacy impact assessment'. This involves assessing any benefits that the information sharing might bring to society or individuals. It also involves assessing any negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. It should help to avoid or minimise the risk of any detriment being caused.

4 The CYPT is comprised of different organisations that have individual governance and legal identities, and the partners the CYPT works with may have their own governance and legal identities. Though all are working to a common purpose, each may be required by their own governance to share certain sorts of information or expressly **prohibited** from sharing certain sorts of information. This document cannot address these individual differences. What is required in every instance is for each organisation to work to the common purpose, to act to promote the wellbeing of children and protect them from harm. In every instance where an individual organisation's process or governance seems to jeopardise this over-riding concept, legal and/or professional advice should be sought.

2. Individual practitioners

A decision by an individual practitioner to share sensitive, personal information about an individual service user with colleagues needs to be made in full awareness of the implications. This is because the unnecessary or inappropriate sharing of this sort of information is more likely to cause damage, distress or embarrassment to individuals. Some information is so sensitive, for example that which may be contained in a health record, that in normal circumstances a patient's explicit consent must be obtained to share or use it for a non-medical purpose.

Guidelines for good practice by individual practitioners

1 Individual practitioners must comply with the good practice guidelines outlined in this document and in the CYPT leaflet, *Information Sharing: A practice guide for CYPT Practitioners and Managers*. In doing so, they can be confident that they are operating within the law and will be fully supported by their employing organisation.

2 Data protection law can require that an individual knows only about the intention to share information about them. It is not always necessary to obtain consent. There are circumstances in which professional concerns about individual safety and the greater public interest will determine that the requirement for consent be waived. The leaflet for service users, *"Information Sharing in Brighton and Hove Children and Young Peoples Trust: what you need to know"*, and the leaflet for staff, *"Information Sharing: A good practice guide for CYPT Practitioners and Managers"*, will help practitioners manage these issues.

3 If you decide that you do need consent to legitimise your processing of information, this must be a specific, informed and freely given agreement. In this context, a failure to object is not consent. Most importantly, the individual must understand what is being consented to and the consequences of giving or withholding consent. If you are **relying** on consent to share information about a person, you **must** stop doing so if consent expires or is withdrawn.

4 It is not justified to share information that identifies people when anonymised information could be used as an alternative. Practitioners should be alert to the possibility of information about third parties not directly involved in the work (relatives, neighbours) finding its way onto records.

3. A broad principle that applies to Organisations and Individual practitioners

Any practitioner or manager using personal information, whether to help a specific family, or to inform wider service development, should regularly review processes to ensure that they are not sharing information that is **not** relevant to achieving the specified objective. **This applies within organisations, within departments, within teams; not just between different organisations**. If only certain departments are involved in providing the service that the information sharing is intended to support, **only** those departments should have access to the information.

4. Child protection and sharing information

"The support and protection of children cannot be achieved by a single agency. Every service has to play its part. All staff must have placed upon them the clear expectation that their primary responsibility is to the child and his or her family". **(Lord Laming in the Victoria Climbié Inquiry Report, January 2003)**.

To provide effective and efficient services, agencies and practitioners need to share personal information, particularly when it would help prevent an individual's life or life chances being

jeopardised. Across the agencies within the CYPT there is a legal duty to prioritise the protection of children and the promotion of their life chances. In some situations practitioners may still feel constrained from sharing personal information by uncertainty about when they can do so lawfully.

When there is evidence or reasonable cause to believe that a child is suffering, or is at risk of suffering, significant harm, or information relates to the prevention of significant harm to a child or serious harm to an adult (including through the prevention, detection and prosecution of serious crime), then sharing confidential information without consent will almost certainly be justified on the basis that it is in the public interest.

Of course it is not possible to give guidance to cover every circumstance in which sharing of confidential information without consent will be justified. You must make a professional judgement on the facts of the individual case. The decision should be taken in accordance with legal, ethical and professional obligations outlined in this document, informed by the practitioner's own experience and expertise, and with the support of their line manager. **The CYPT has a commitment to information sharing and practitioners can have confidence in the continued support of their organisation where they have used their professional judgement and shared information professionally**.

It is hoped this guidance will be useful in supporting early intervention and preventative work where decisions about information sharing may be less clear than in safeguarding or child protection situations. However where the information being considered relates to clear child protection concerns practitioners from all agencies should be in no doubt that there are no insurmountable legal barriers to sharing information appropriately, and a demonstrably proportionate sharing of information can be justified as being in the public interest. This principal applies across the agencies, and is line with all professional ethical codes.

There may be other cases where you will be justified in sharing limited confidential information in order to make decisions on sharing further information or taking action – the information shared should be necessary for the purpose and be proportionate. Remember that the piece of information you hold represents part of a jigsaw puzzle, the degree of its significance may only be clear to a social worker with a much fuller picture of the background and concerns for this child.

You should record your decision and the reasons for it, whether or not you decide to share information. If the decision is to share, you should record what information was shared and with whom.

If you are in any doubt about whether to share information seek advice. Do not fail to share the information because you are concerned about the possibility of a complaint at a later date. Your organisation will support you if you can demonstrate your approach was reasonable in the circumstances. No review into inter agency working has ever criticised practitioners for sharing too much information regarding child protection concerns. The reverse is the case, often with potentially devastating consequences for the child, but also for the practitioner.

"Peter was seen with Ms A by his GP on 26thJuly 2007. The GP has said subsequently that he had considerable misgivings about Peter's appearance and demeanour at that appointment. He felt Peter was in "a sorry state". However, he did not take any action to alert others to his concern. He assumed that others would have similar concerns and would be in a better position to take action…"*

(*this is a week before his death, three days before legal advice concluded there were insufficient grounds for care proceedings at that time)

Executive Summary,
Serious Case Review: Baby Peter 2009

2. Fairness and transparency

The law says:

Personal information shall be processed fairly. The processing won't be fair unless the person has, is provided with, or has readily available:

- information about your identity and that of the organisation that will process the information
- information about the purpose the information will be processed for, and
- any other information necessary to enable the processing to be fair.

Guidelines for good practice

1 A privacy notice (previously called a Fair Processing notice) is a blanket way of informing people how information will be shared and what it will be used for. Each school in Brighton and Hove, for example, has its own privacy notice which informs parents about data which is shared with the CYPT and why. For the CYPT itself, while it is not labelled a privacy notice, the leaflet for service users, *"Information Sharing in Brighton and Hove Children and Young Peoples Trust: what you need to know"*, is intended to be given at first contact and performs this function. The CYPT does not yet have an on-line privacy notice.

2 Fair processing is a **pro-active** function, not a retrospective response to a request. Privacy notices must be accessible and targeted at a particular audience. While the leaflet referred to above is good enough for general application, the linguistic and cognitive ability of an individual service user may mean that they do not understand it and another way needs to be found to convey the message. In the same way, the manager of any specific project or initiative must check whether what they are doing requires its own privacy notice.

Giving leaflets to individual service users is one way forward. It is also good practice to provide fair privacy notices to people when, for example, you hold public meetings with them or you send out general letters about your service.

3 The CYPT will review its fair processing information regularly to make sure that it still provides an accurate description of the information sharing being carried out. Individual managers and practitioners must also regularly review whether the information provided to service users is still an accurate representation of their local or individual practice and, if not, take appropriate steps to address the issue.

4 Service users will sometimes have questions about how information about them is being managed, or may object to information being shared. Practitioners should engage with such matters head on, always discuss them in supervision, seek guidance from their manager and, where it is appropriate, offer specific meetings to seek to resolve the issue. Where the issue becomes a formal complaint there are existing processes to follow. Managers of service units should ensure that a record of emerging significant themes around information sharing is kept and passed on up to inform wider CYPT learning about information sharing.

5 There are circumstances when it is legitimate to share information without a person's knowledge or consent. This might be the case where a failure to share information about a parent's lifestyle could put a child at risk. There are also other situations where information could be shared despite a lack of consent; for example, where the sharing is necessary to safeguard public safety in an emergency situation. In many criminal justice contexts it is not feasible to get consent, because doing so may prejudice a particular investigation. However, you should be prepared to be open with the public about the sorts of circumstances in which you may share information without their knowledge or consent. The leaflet for service users, *"Information Sharing in Brighton and Hove Children and Young Peoples Trust: what you need to know"*, makes this clear.

3. Information standards

The law says:

Information shall be adequate, relevant, not excessive, accurate and up to date.

Guidelines for good practice

1 Check the quality of information before it is shared to minimise the spreading of inaccuracies across information systems. In individual casework, a simple device would be to ask the subject to check the quality of information. This could form part of the consent process.

2 Where large amounts of information are being processed, such as in a project, it is usually not possible to check the accuracy of every record. In such circumstances a sample of records should be checked. If necessary, cautionary notices to advise about potential errors should be circulated to project staff and mechanisms agreed to resolve information quality problems.

3 Be alert to variations in data recording practice. For example, a person's date of birth, or even name, can be recorded in various formats. This can lead to records being mismatched, duplicated or corrupted. Before sharing information you must make sure that the organisations and partners involved have a common way of recording key information.

4 Having a clearly defined objective will help us determine what information is necessary to achieve that objective. We will thus be able to justify seeking and sharing that information. We must **never** share information if it is not necessary to do so. It is good practice for both practitioners and managers to check every now and then that all the information being shared still meets the criteria. Experience and professional judgement are key determining factors and, if there is any doubt, practice concerns should always be raised in supervision or with a manager.

5 The spreading of inaccurate information across a network can cause significant problems for individuals. If you believe that you have shared inaccurate information, you should first take steps to determine what is accurate. Once content that the information you have is now accurate, you should ensure that it is corrected by others holding it. In cases of continuing disagreement between organisations about the accuracy of a record, the matter should be taken to the appropriate senior manager.

4. Retention of shared information

The law says:

Personal information shall not be kept for longer than is necessary.

Guidelines for good practice

1 Constituent organisations within the CYPT have their own guidelines governing the retention of information, depending on the purpose and the nature of the work engaged in. For example, the rules for the retention of information by social services specify one period of time for children who have a child protection plan, another for children who have been looked after, and yet another for children who are adopted. There are rules which determine when such records containing that information are archived, when and by whom they can then be accessed, and when they should be destroyed. Each other constituent part of the CYPT has its own agreed timescales and processes.

South Downs Health staff working for the CYPT have access to Part 2 of Records Management: NHS Code of Practice. This contains a complete list of retention periods for NHS records. There is a link to this document in Appendix 4.

The default position will always be to retain information according to individual organisations' policy – in the full knowledge that this may mean that the professional partners working with a family or on a wider project will retain information for different durations. Care should be taken that the consent process or the fair processing process leaves the service user clear about the length of time their records will be kept by different organisations.

Where there are no specified rules about information retention, professional judgement will need to be exercised.

Considerations for judging retention periods include:

- the current and future value of the information for the purpose for which it is held;
- the costs, risks and liabilities associated with retaining the information; and
- the ease or difficulty of making sure the information remains accurate and up to date.

2 Retention policies should be reviewed annually as part of the organisation's governance process. If, for example, it is clear that retained records are not being subsequently used, this would call into question the need to retain them. The rigour of this review should be subject to the annual Quality and Performance Audit.

In individual cases staff must rely on experience and professional expertise to come to a balanced decision about whether to retain or delete the information. If this is at variance with the existing unit policy, it must be discussed in supervision or managerial guidance sought.

3 There is a significant difference between permanently, irreversibly deleting a record and merely archiving it. If you merely archive a record or store it 'off-line' it must still be necessary to hold it and you must be prepared to give subject access to it and comply with the data protection principles. If it is appropriate to delete a record from your live system you should also delete it from any back-up of the information you keep.

4 Outside individual casework, organisations sharing bulk information, irrespective of whether this is within or without the CYPT, should have an agreement about what should happen once the need to share the information has passed. In some cases the best course of action might be to return the shared information to the organisation that supplied it without retaining a copy. In other cases it may be appropriate for all the organisations involved in a project to delete their copies of the information.

In some situations where there is a reluctance to lose valuable data, it may be worth considering whether anonymising the information may meet the need.

5. Security of shared information

The law says:

Personal information shall be protected by appropriate technical and organisational measures.

Guidelines for good practice

1 Access to personal information should be on a strict need-to-know basis. Only staff who need access to personal identifiable information should have access to it, and they should only have access to the information items that they need to see. Though most offices of the CYPT have a security presence, members of the public or outside contractors can and do come into our offices. Outside normal working hours cleaning and maintenance staff have free access to unsupervised office areas. The following rules apply to all staff:

- Personal files must **never** be left unattended or unsupervised. This means that, outside normal working hours, they **must** be locked away in cabinets.

- Codes for accessing computers must **never** be noted in such a way that others can see and use them

- The conveying of information needs to be achieved in a secure way. The Post Office offers some security in the registered post service; the council's courier system can be regarded as secure, providing items are sealed and appropriately marked; the council e-mail system is currently awaiting approval to link to the Government Connect network which will guarantee secure links across all local authorities, NHS, Police, Criminal Justice and Central Government Agencies. Until this system is agreed and a list of secure connections is published, staff cannot assume that anything other than intranet connections or connections to South Downs Health sites are secure enough, and e-mail should not be the medium of choice.

- The council's effective intranet system means that information can be easily received or delivered by a large number of employees. But it can just as easily be misdirected. Before pressing the "Send" button, staff should ensure that the list of addressees is correct. It is very common for the system to default to staff with same first or second names and for the wrong recipient to get the information.

2 The CYPT and external partners can have different standards of security and different working cultures. We are still in the process of establishing a common security standard. Until that is achieved, practitioners and managers should always address any security issues and seek a common way forward before sharing any personal information.

Primary responsibility for ensuring that shared information will continue to be protected by adequate security once other organisations have access to it sits with the organisation holding the information initially. There should be clear agreement about who is allowed to access and who is allowed to alter a record.

3 The CYPT Training Consortium is developing an Information Sharing module which will be part of the Core Skills and Knowledge and Induction programmes.

6. Access to personal information

The law says:

Individuals have a right of access to information about them.

Guidelines for good practice

1 Whether engaging with groups of service users or working with an individual, it is good practice to identify a single point of contact for people to go to when they want to access their information, and to make people aware of this facility as a part of Fair Processing or the consent process.

2 The CYPT is required by law to enable people to access information held about them. The CYPT and SDHT have different processes and policies and staff will need to follow the appropriate one. Best practice would be to show service users their records at the point of engagement.

3 Though the CYPT is one service delivery organisation, it is comprised of different parts, each of which may hold its own records about the same individual. Good records management practice will need to be developed in which each organisation keeps a brief record of where other information is held. This will make it easier for the CYPT to locate all the information held about a person when an access request is received.

When the CYPT receives a request for personal information, it is required by law to explain why the information is held, and to whom it has been supplied. It is also required to provide the individual with any details we have about the provenance of the information. Care should be taken that, when information has been supplied to us in confidence, that this confidence is not broken.

4 In rare instances, practitioners may feel that it is not in the public interest for a service user to access some information held about them. The rough yardstick for gauging this is to think about the effect that releasing the information would have on the individual or a vulnerable other. Appendix 5, Guidance on exemption to subject access to records, gives more detail. In every instance where the right way forward is unclear, further help should be sought in supervision or from a manager and, where appropriate, a legal advisor

7. Freedom of Information

The law says:

The Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 give everyone the right to ask for information held by a public authority, to be told whether the information is held, and, unless exempt, to have a copy of the information.

Guidelines for good practice

1 Service users or citizens may sometimes make requests for information that is partially personal and partially non-personal. For example, a person may request information about them that is being shared between various agencies, and ask for information about those agencies' policies for sharing information. CYPT Staff should be aware that, while they will be required to deal with the personal information, in the question of policies they need to refer to their employing organisation's Freedom of Information publication scheme.

2 Brighton and Hove City Council's scheme is managed by:

The Freedom of Information Team
Hove Town Hall
Hove, East Sussex
BN3 4AH
Email: freedomofinformation@brighton-hove.gov.uk

South Downs Health Trust's scheme is managed by:

The Information Governance Coordinator
South Downs Health
Brighton General Hospital
Elm Grove, Brighton
BN2 3EW
Email: enquiry@southdowns.nhs.uk

8. Review

The law says:

Nothing specific about reviewing information sharing processes.

Guidelines for good practice

1 Integrated working will not be effective unless information is shared appropriately across professional partners. It therefore make sense to regularly review whether our sharing of information is having the desired effect. Managers should ensure that, in their reviews of their team's performance, they consider:

2 Whether the sharing of information practices are making a positive difference for the service users.

3 Whether any privacy notices still provide an accurate explanation of the information sharing activity.

4 Whether the procedures for ensuring the quality of information are working in practice.

5 Whether the other organisations they are sharing information with are also meeting agreed quality standards.

6 Whether record retention periods are being adhered to and continue to reflect business need.

7 Whether security arrangements are adequate and, if not, whether any security breaches have been investigated and acted upon.

8 Whether individuals are being given access to all the information they are entitled to, and that they are appropriately supported to exercise their rights.

9 When assessing your information sharing it is also important to consider any complaints or questions that you have received from members of the public.

APPENDICES

Appendix 1

Key Information Sharing materials

For service users:

- CYPT LEAFLET – *Information Sharing in Brighton and Hove Children and Young People's Trust: what you need to know*

For every practitioner and manager:

- CYPT LEAFLET – *Information Sharing: A practice guide for CYPT Practitioners and Managers*
- DCSF BOOKLET – *Information Sharing: Pocket Guide*
- CYPT HANDOUT – *Seven Golden Rules for Information Sharing*
- CYPT HANDOUT – *Flowchart of key questions for Information Sharing*

For every office:

- CYPT POSTER – *Seven Golden Rules for Information Sharing*
- CYPT POSTER – *Flowchart of key questions for Information Sharing*
- DCSF PUBLICATION – *Information Sharing: Guidance for Practitioners and Managers*
- CYPT BOOKLET – The Code of practice for Information Sharing in Brighton and Hove Children and Young People's Trust

Appendix 2

Example of a simple information sharing procedure

Procedure for sharing information between Newtown Constabulary, Reporter to the children's panel and social work departments.

1. Contact details

Named individuals in Council Social Work departments and Area Children's Reporters.

2. Types of information

2.1 Child Protection Initial Report Form NM/59/2 to be sent to appropriate Social Work Department and Children's Reporter. These will be marked CONFIDENTIAL.

2.2 Memoranda as required. These will always be marked CONFIDENTIAL.

2.3 Crime reports may also be disclosed.

2.4 Verbal information will be shared at case conferences. This information will be either RESTRICTED or CONFIDENTIAL. Minutes should be classified according to the value of information in them.

3. How to handle the information

3.1 Transmission

3.1.1 RESTRICTED information can be transmitted over the telephone or sent by fax. CONFIDENTIAL information must be sent in a double envelope with the protective marking shown on the inner one.

3.2. Storage

3.2.1 All information must be kept under lock and key when not in the personal custody of an authorised person. The "need-to-know" principle will be strictly enforced. CONFIDENTIAL information needs to be protected by two barriers, for example, a locked container in a locked room.

3.3. Release to third parties

3.3.1 No information provided by partners to these procedures will be released to any third party without the permission of the owning partner.

Appendix 3

Guidance available from the Information Commissioner at www.ico.gov.uk

- Sharing personal information: Our approach. (A general position paper on information sharing.)
- Data sharing between different local authority departments.
- The use and disclosure of information about business people.
- The Crime and Disorder Act 1998: data protection implications for information sharing.
- Sharing information about you. (Advice to the public about information sharing.)

Appendix 4

Other sources of advice and guidance

Audit Commission:
www.audit-commission.gov.uk

Cabinet Office:
www.cabinetoffice.gov.uk

Chief Information Officer Council:
www.cio.gov.uk

Communities and Local Government:
www.communities.gov.uk

Department for Children, Schools and Families:
www.dfes.gov.uk

Department of Health:
www.dh.gov.uk

Essex Trust Charter:
www.essexinformationsharing.gov.uk

Improvement Service:
www.improvementservice.org.uk

London Connects:
www.londonconnects.gov.uk

Ministry of Justice:
www.justice.gov.uk

National Archives:
www.nationalarchives.gov.uk

Public Record Office of Northern Ireland:
www.proni.gov.uk

Records Management Society:
www.rms-gb.org.uk

Society of Archivists:
www.archives.org.uk

The Scottish Government:
www.scotland.gov.uk

Confidentiality: NHS Code of Conduct
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

Records Management: NHS Code of Practice
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

Appendix 5

Guidance on exemption to subject access to records

Health Order

The Data Protection (Subject Access Modification) (Health) Order 2000, known as "the Health Order", allows for an exemption to the right to subject access. NHS patients can be denied access to all or part of their health records if one of the following conditions applies:

- if, in the opinion of the *appropriate health professional*, giving access would disclose information likely to cause serious harm to the physical or mental health or condition of the patient or to any other person (for example, a child in a child protection case)

- if giving access would disclose information which could identify a third party (unless the individual concerned has given their consent).

A health professional means a registered practitioner from a medical or allied profession, including medical practitioners, dentists, opticians, pharmacists, nurses, midwives, health visitors, osteopaths, chiropractors, chiropodists, clinical psychologists, child psycho¬therapists, speech therapists, occupational therapists, physio¬therapists, etc.

The appropriate health professional means one of the following:

- the health professional who is currently (or was most recently) responsible for the clinical care of the data subject in matters relating to the subject access request

- where there is more than one such health professional, the one who is the most suitable to advise on matters relating to the subject access request

- failing that, a health professional who has the necessary experience and qualifications to advise on matters relating to the subject access request.

Education Order

The Data Protection (Subject Access Modification) (Education) Order 2000, known as "the Education Order", allows an education authority to deny access to all or part of an education record if one of the following conditions applies:

- if giving access would disclose information likely to cause serious harm to the physical or mental health or condition of the data subject or to any other person

- if giving access would reveal that the data subject may be at risk of child abuse.

Social Work Order

The Data Protection (Subject Access Modification) (Education) Order 2000, known as "the Social Work Order", allows a local authority or NHS Trust to deny access to all or part of a social care record if the following condition applies:

- if giving access would be likely to prejudice the ability to carry out social work because disclosure would be likely to cause serious harm to the physical or mental health or condition of the data subject or to any other person.

"It is important for professionals to trust their feelings when they perceive children to be suffering, and not make assumptions that others have also perceived it and are better placed to act. It is simpler to lift the telephone than to live with the regret of not having done so."

Serious Case Review: Baby Peter
Executive Summary
LSCB Haringey
February 2009
Paragraph 4.3.6

First Edition: September 2009

Translation? Tick this box and take to any council office.

Arabic ❑ ترجمة؟ ضع علامة في المربع وخذها إلى مكتب البلدية.

Bengali ❑ অনুবাদ? বক্সে টিক চিহ্ন দিয়ে কাউন্সিল অফিসে নিয়ে যান।

Cantonese ❑ 需要翻译？請在這方格內加剔，並送回任何市議會的辦事處。

Farsi ❑ ترجمه؟ لطفاً این مربع را علامتگذاری نموده و آن را به هر یک از دفاتر شهرداری ارائه نمائید.

French ❑ Traduction? Veuillez cocher la case et apporter au council.

Mandarin ❑ 需要翻译？请在这方格内划勾，并送回任何市议会的办事处。

Polish ❑ Tłumaczenie? Zaznacz to okienko i zwróć do któregokolwiek biura samorządu lokalnego (council office).

Portuguese ❑ Tradução? Coloque um visto na quadrícula e leve a uma qualquer repartição de poder local (council office).

Turkish ❑ Tercümesi için kareyi işaretleyiniz ve bir semt belediye burosuna veriniz

other (please state) ❑

This can also be made available in large print, Braille or on audio tape

2576 design by www.graphicdesignteam.org.uk