DATA PROTECTION ACT 1998

GUIDANCE TO SOCIAL SERVICES

March 2000
CONTENTS

Section 1  Introduction  4

Section 2  Glossary of terms  8

Section 3  Good practice in record keeping  14

Principles underpinning good practice  14
A policy framework  15
Retention and destruction of records  16
Records subject to statutory requirements  17
Management commitment to good practice  17
### Section 4  
**Details of the Act and its implementation**  
20

### Section 5  
**Access to social services records**  
24

- Personal information covered by this guidance  
- Right of access  
- Requests by, or on behalf of, a child or a young person under 18  
- Requests made on behalf of an adult lacking mental capacity  
- Requests made through another person (an agent)  
- Requests for access to the records of a deceased person  
- Dealing with a request for access, and fees  
- Where an authority does not hold the information requested  
- Points to consider before access is given  
- Information to be disclosed  
- Information that includes details about another person  
- Timescale  
- Presenting the information  
- Where an authority holds information that the person considers is inaccurate  
- When an authority can rely on an exemption to refuse access  
- Where an authority decides to refuse access
Section 6  Confidentiality of social services records 34

General Principles 34

Disclosing personal information:
  With consent 35
  Without consent 36
  - for social services purposes 37
  - for other purposes 37

Disclosure of information about those without capacity to consent 38

Sharing information 38

Disclosure of information for research purposes 39

Monitoring 39

Appendix 1  The Data Protection Principles 40

Appendix 2  The Data Protection (Subject Access Modification) (Social Work) Order 2000
  - Explanatory Note 41

Appendix 3  Data Protection Advisory Group 43
1.1 The Data Protection Act 1998 (DPA) came into force on 1 March 2000. The purpose of this guidance to local authority social services is to provide information about how the DPA works in relation to giving access to social work records. The guidance also gives:

- guidance on good practice in compiling and maintaining records. Authorities having well-maintained records will find it easier to comply with the requirements of the Act;
- advice on the need for policies covering the retention and disposal of other records;
- guidance on confidentiality and social services records;

1.2 The DPA repeals the Data Protection Act 1984. It also repeals the Access to Personal Files Act 1987 and most of the Access to Health Records Act 1990. The effect is to create a single regime of access for social work records. Some of the DPA's provisions are subject to transitional arrangements. The DPA enhances the rights of individuals to gain access to information held about them. The responsibilities of the Data Protection Commissioner (DPC) (formerly the Data Protection Registrar) are extended, not only in terms of scope but also functions...
and enforcement. The DPC has published guidance on how the Act may be interpreted, entitled *The Data Protection Act 1998 – An Introduction*, which can be ordered from the DPC’s office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or through the information line on 01625 545 745. It is also available on the internet at www.dataprotection.gov.uk.

1.3 **Section 2** provides a glossary of terms used in this guidance, including a list of definitions from the DPA.

1.4 **Section 3** of this guidance provides good practice guidance on record keeping. **Section 4** gives details about the DPA and its implementation. **Section 5** deals with the rights of access and rights of appeal under the DPA, by the people who are the subject of the information, in relation to personal information that authorities hold for the purpose of their social services functions. **Section 6** deals with confidentiality and the circumstances in which people other than data subjects may be given access to personal information held by an authority.

1.5 On the date that this guidance comes into effect it will replace the following guidance which is then withdrawn:

- LAC(87)10 – Data Protection (Subject Access Modification) (Social Work) Order 1987
- LAC(88)17 – Personal Social Services: Confidentiality of Personal Information
Enquiries

1.6 This document is not meant to be a substitute for the Act itself, and in cases of doubt authorities should consult their legal advisers. Enquiries about the general application of the DPA should be made to the Data Protection Commissioner (details given in paragraph 1.2 above).

1.7 Other enquiries may be addressed, in writing, to:

The Department of Health
Social Care Group 2A
Area 624
Wellington House
133-135 Waterloo Road
London SE1 8UG
Glossary of terms

Where an italicised reference follows a definition given below, this indicates that the definition in question comes from that provision of the Data Protection Act 1998.

In the guidance generally an italicised reference is to that section of or Schedule to the 1998 Act.

**Accessible record**
includes health records and accessible public records.
(Section 68(1))

**Accessible public record**
means any record which is kept by an authority specified as a local social services authority and is a record of information of a description held for any purpose of the authority's social services functions.
(Section 68(1)(c) and Schedule 12)

**Agent**
means a person authorised expressly by the data subject to act on his or her behalf.
Authority

means a local authority's social services department.

Case record

means all the records held by a social services department about a person for whom they have provided or are providing services.

Data

means information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;

(d) does not fall within (a), (b) or (c) above but forms part of an accessible record.

(§ 1(1))

Data controller

means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

(§ 1(1) and (4) and § 63)
Data processor
in relation to personal data, means any person (other than an employee of the
data controller) who processes the data on behalf of the data controller.
(section 1(1))

Data subject
means an individual who is the subject of personal data.
(section 1(1))

DPA

DPC
means the Data Protection Commissioner.

Health Professional
means:
(a) a registered medical practitioner,  
(b) a registered dentist as defined by section 53(1) of the Dentists Act 1984  
(c) a registered optician as defined by section 36(1) of the Opticians Act 1989  
(d) a registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act 1954  
(e) a registered nurse, midwife or health visitor  
(f) a registered osteopath as defined by section 41 of the Osteopaths Act 1993  
(g) a registered chiropractor as defined by section 43 of the Chiropractors Act 1994  
(h) any person who is registered as a member of a profession to which the Professions Supplementary to Medicines Act 1960 for the time being extends  
(i) a clinical psychologist, child psychotherapist or speech therapist  
(j) a music therapist employed by a health service body, and  
(k) a scientist employed by such a body as head of a department
(section 69)

Health record
means any record which -  
(a) consists of information relating to the physical or mental health or condition of any individual, and  
(b) has been made by or on behalf of a health professional in connection with the care of that individual.
(section 68(2))

Local Social Services Authority
means any authority which, by virtue of section 1 or 12 of the Local Authority Social Services Act 1970, is or is treated as a local authority for the purposes of that Act.
Obtaining or recording
in relation to personal data, includes obtaining or recording the information to be contained in the data.
(section 1(2)(a))

Personal data
means data which relate to a living individual who can be identified:
(a) from those data, or
(b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller, and includes any expression of opinion about the individual, and any indication of the intentions of the data controller or any other person in respect of the individual.
(section 1(1))

Processing
in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
(a) organisation, adaptation or alteration of the information or data;
(b) retrieval, consultation or use of the information or data;
(c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
(d) alignment, combination, blocking, erasure or destruction of the information or data.
(section 1(1))

Recipient
means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular enquiry by or on behalf of that person made in the exercise of any power conferred by law.
(section 70(1))

Relevant filing system
means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
(Section 1(1))
Relevant person

means one of the persons referred to in article 7(2) of the Data Protection (Subject Access Modification) (Social Work) Order 2000 and includes local authority social services staff.

Sensitive personal data

means personal data consisting of information as to -
(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Social Services functions

means the functions conferred upon a local social services authority by virtue of the Local Authority Social Services Act 1970.

Third party

in relation to personal data, means any person other than
(a) the data subject
(b) the data controller
(b) any data processor or other person authorised to process data for the data controller or processor

Using or disclosing

in relation to personal data, includes using or disclosing the information contained in the data.

(Section 70(1))
Good practice in record keeping

Principles underpinning good practice

3.1 Good case recording helps to focus the work of social services staff and supports effective partnerships with service users and carers. It ensures that there is a documented account of their involvement with individual service users, families and carers. It assists continuity when workers are unavailable (or change) and provides an essential tool for managers to monitor work. It is a major source of evidence for investigations and enquiries. Over the past 25 years, inadequate case records have often been cited as a factor in cases with tragic outcomes.

3.2 Best practice in recording is based on key principles of partnership, openness and accuracy. Effective recording is part of the total service to the user. Social services departments need to give staff clear guidance and training which promotes working in partnership with service users and carers. This includes constructing and sharing written records. Gaining clearance to share information provided by another person with service users in the normal course of day-to-day work is an important way of ensuring that access to records is maximised.

3.3 Social services staff should tell service users why and when information is to be transferred or exchanged between different parts of the service and with provider
agencies. They should secure their agreement to this process and ensure that this is clearly recorded. This is an important aspect of people’s rights and should mean that when service users have access to their records the contents are not a surprise.

3.4 Working in this way should promote greater accuracy in recording. Fact will need to be distinguished from opinion; issues discussed, the action agreed and the reasons for decisions made, all should be succinctly recorded.

A policy framework

3.5 Social services departments should have a policy framework which expresses the values and principles underpinning recording practice. Policies should ensure that the Data Protection Act is fully implemented in the way the department records and shares information. Policies should cover the following issues:

• A statement of purpose of recording, overall commitment to shared records, and equality of opportunity issues.
• A definition of documents to be routinely copied to users.
• Statements of access including users with special needs, confidentiality and exceptions/restrictions.
• Public information on social services policy and practice.
• Agreements on information provided by other persons or agencies – eg health, housing, Police, Benefits Agency.
• Contracts with providers and expectations of records to be maintained.
• Agreements on the use of social services records by other agencies.
• The retention and destruction of records, electronic and manual systems.

3.6 Information on individual service users may be held in a number of different locations, by both commissioners and providers. In essence, all records on one individual, held by social services, form the record of the department’s involvement with that individual. When access is requested, it is important to ensure that this is arranged when the information is held in different locations.

3.7 Policies on case recording should ensure that staff are given guidance on the structure of files and the maintenance of separate files for individual service users. Guidance should be given to staff on how these policies operate in practice. Social services IT strategies need to be explicitly linked with case recording policies and procedures. Cross referencing between paper based records and those held on IT systems is essential. Staff need to be encouraged to develop IT skills which can enhance their service to users and carers.

Retention and destruction of records

3.8 The DPA requires that personal data shall be: adequate, relevant and not excessive for the purpose(s) for which they are held (the third principle); accurate and where necessary kept up to date (sixth principle); and not kept for longer than is necessary for its purpose(s) (fifth principle). (See Appendix 1 for details of the data protection principles.) These three combined require authorities to introduce procedures covering the review of information held on files, especially where sensitive personal information is held as part of the record and there are issues of confidentiality. Such procedures include the establishment of a policy covering the retention and destruction of records.

3.9 This should recognise any legal requirements governing the length of time during which records need to be retained, be compatible with document management policies and, especially where there is a requirement to retain records for extended periods (eg adoption records, for research) be discussed with the authority’s archivist. Where no legal requirement to retain information beyond the closure of the record exits the authority will need to establish its own retention periods. Normally personal information should not be held for longer than 6 years after the subject’s last contact with the authority.

3.10 Exceptions to this period will occur when records:

• need to be retained because the information contained in them is relevant to legal action which has been started;
• are required to be kept for longer by statute;
• are archived for historical purposes;
• consist of a sample of records maintained for the purpose of retrospective comparison;
• involve the transfer of significant information, with subject identification, on to aggregated files;
• relate to individuals and providers of services who have, or whose staff have been judged unsatisfactory;
• are held in order to provide, for the subject, aspects of his/her personal history.

3.11 It is the responsibility of the authority’s legal department to provide information on pending legal action. If such action is pending a note should be appended to the file confirming that the records should not be destroyed.

The following records are subject to statutory requirements:

• Case records relating to children who have been placed, to be retained until the 75th anniversary of the child’s birth or for 15 years after death if the child dies before age 18 (Arrangements for placement of Children (General) Regulations 1999).
• Records relating to a foster parent or other person and any entry relating to him in a register must be retained for at least 10 years from the date on which his approval is terminated or until his death, if earlier (Foster Placements (Children) Regulations 1991).
• A video recording of a child witness made under the Criminal Justice Act 1991 must be retained for so long as it may be needed for the purpose of a trial or appeal. The decision to destroy it must be jointly by the Director of Social Services and the senior police officer concerned (Code of Practice for Video Recorded Interviews with Child Witnesses for Criminal Proceedings 1991 (paragraph 3.14)).
• Registered Residential Homes are required to keep records for 3 years after the date of the last entry (Registered Care Home Regulations 1984, Regulation 6(4)).
• Registered Nursing Homes are required to keep case records for not less than 1 year after the date the individual ceases to be a patient in the home. But the Mental Health Act 1983 requires records to be kept for 5 years after the date the person ceases to be a patient in the home (Nursing Homes and Mental Nursing Homes Regulations 1984, Regulations 7(6) and (10)).

Management commitment to good practice

3.12 In addition to a policy framework which expresses the values and principles underpinning recording practice, staff will need guidance on best practice in case recording. This should cover the style of recording, the content of records to be maintained, and the degree of oversight that will be exercised by managers. Guidance on recording should cover specific requirements, for example child protection and looked after children records. Case records will need to contain evidence of the assessment and a statement of objectives for the work to be done. There should be a balance between running records and periodic summaries and reviews. Records should show evidence of how information has been shared with
the user and access to records promoted. This could include copies of key records being given to the user or signatures on file to show that these have been discussed with the user. Quality standards for recording should give guidance to staff on how they can encourage active involvement in assessment and recording, whatever the abilities and skills and language of the service user may be.

3.13 Social services managers need to demonstrate a commitment to case recording as an important part of the service to users and carers and to ensure that policy and procedures are established. The commitment should be explicit and reflected in recruitment, induction, training, performance appraisal, auditing, monitoring and review. In departments where this happens, and particularly where random routine auditing of case records takes place, there is evidence that standards of case recording do improve.

3.14 Throughout the process of assessment and intervention and the writing of the record, management oversight should support work and ensure accountability. Decisions made in supervision are a significant part of the record for service users and they should be clearly recorded and held on the main case file as an integral part of the record.
4.1 The DPA implements the European Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive) which came into force on 24 October 1998. The DPA also gives effect to the judgement of the European Court of Human Rights in the 1989 case Gaskin v the United Kingdom concerning the right of access to social work records.

4.2 The DPA will eventually apply to all personal data, no matter when compiled, that fall within the relevant definitions in section 1(1) of the Act. Personal data include data held in electronic form, and data held in a “relevant filing system” i.e. in structured manual files (see glossary for definition). Most importantly for local authority social services departments, it also includes manual data which form part of an “accessible record” (see glossary and section 68 and Schedule 12).

4.3 The DPA’s full requirements will be implemented subject to transitional periods, which are provided for by the EU Directive. The first transitional period ends on 23 October 2001; the second runs from 24 October 2001 until 23 October 2007. (Schedule 8, paragraph 1(1))
4.4 Existing manual records generally are not subject to the DPA at all during the first transitional period. However, this exception does not apply to existing manual social work records.

4.5 In the first transitional period, in respect of existing manual case records, the subject access provisions of the DPA apply, irrespective of when the information was recorded. The combined effect of the definitions of data held in a “relevant filing system” or which form part of an “accessible public record” covers the kinds of manual records to which Schedule 1 to the Access to Personal Files Act 1987 applied. (The 1987 Act is now repealed.)

4.6 The DPA sets out eight principles of data protection. These are listed in Schedule 1 Part I and interpreted in Schedule 1 Part II of the DPA. These principles limit the reasons for which personal data may be obtained and specify how they may be used. The first principle is also the subject of Schedules 2 and 3 of the DPA. Schedule 2 specifies the conditions relevant for the purposes of fair and lawful processing any personal data; while Schedule 3 specifies the conditions relevant to the processing of sensitive personal data. The principles are reproduced in Appendix 1 of this guidance.

4.7 In some cases local authorities will need to continue to deal with applications made either under the DPA 1984 or the Access to Personal Files Regulations 1989 where these were made before the DPA commenced. Further transitional provision for such cases is made in the DPA. (Schedule 14, paragraph 3 and paragraph 19.)
4.8 The second transitional period applies to certain manual data held in social services records immediately before 24th October, 1998. Exemption provided during the second transitional period covers compliance with the second, third, fourth and fifth principles; the powers of the courts to order rectification, erasure etc; and the first principle except for the requirement to provide the data subject with information as to the identity of the controller and the purposes for which the data are to be processed. (Schedule 8, paragraph 14)

4.9 The transitional periods do not apply to personal data where the processing, whether by manual or automated processes, did not commence until after 24 October 1998. All such ‘new processing’ is subject to DPA from the moment processing commences. Authorities are reminded that “processing” as used in the DPA includes storage of data in any form (see glossary for definition).

4.10 This guidance is concerned with the operation of the DPA during the first transitional period, to 23 October 2001. Further guidance will be issued if needed, before the commencement of the second transitional period on 24 October 2001.
5.1 This guidance covers personal data held electronically, or in “relevant filing systems” or in “accessible public records” (see glossary). In other words, this guidance covers information held about a particular individual by a local social services authority for the purpose of the authority’s social services functions, irrespective of when the information was recorded.

5.2 Where joint records are held, for example in the case of community mental health teams, the relevant organisations, ie the social services department and NHS Trust, will each be required to notify separately, as each is a data controller in its own right. However, the data subject should not have to apply to both organisations for access to their records. Either organisation can provide access to the joint record provided the data subject is informed that the data are held jointly. Authorities and their partners in joint record holding will therefore need to have procedures in place to ensure that the data subject is aware that he/she is not obliged to apply to all partners for access and to inform each other that access has been given.
5.3 The term “joint records”, as used above, does not include records held separately by authorities and other organisations which contain information provided by either organisation to the other. While the information held on each organisation's separate records may be similar, they would not be considered “joint records”. The parties to such exchanges are data controllers in their own right. In such cases data subjects requiring access must make separate applications to each controller.

Right of access

5.4 Subject to a limited number of exemptions made under Part IV of the DPA, any living person who is the subject of personal information held and processed by a social services authority has a right of access to those data. The information comprising this data includes factual information, any expressions of opinion, and the intentions of the authority in relation to the individual. Where access is refused, the data subject may appeal to the courts or the Data Protection Commissioner.

5.5 A person does not have the right to know what is recorded about someone else. So, for example, where an authority has maintained files on an entire family and a request is recorded for access to one of these “family” files, one member is not entitled to see information about another member without that person's consent. However, there may be circumstances in which the local authority considers it reasonable to disclose such information without consent (see paragraphs 5.7 and 5.23).
5.6 In circumstances where disclosure of the data requested is not possible without disclosing information about another person, normally the request need not be complied with unless the other person has given consent to the disclosure. This does not excuse the controller from providing as much of the information sought as can be disclosed without revealing that person's identity, whether by omission of names or other identifying particulars. However, there may be occasions where it is ‘reasonable in all the circumstances’ to comply without that other person's consent. This includes the disclosure of identifiable details about a “source” who has contributed information to a social services record.

5.7 When disclosing information which identifies another person without that person's consent, in determining what is ‘reasonable in all circumstances’ to comply with the request it is necessary to have regard to:

- any duty of confidentiality owed to that other person;
- any steps taken with a view to seeking consent of the other person to the disclosure;
- whether the other person is capable of giving consent;
- any express refusal of consent by the other person.

(Section 7(4))

Requests by, or on behalf of, a child or a young person under 18

5.8 The right of access extends to children and young people under 18 who understand what it means to exercise that right. Where a child or young person under 18 makes a request for access to their records, an authority will need to decide whether or not he or she has sufficient understanding to do so. That is, does he or she understand the nature of the request? If so, then the request for access should be complied with.

5.9 If a child or young person under 18 does not have sufficient understanding to make his or her own request, a person with parental responsibility (referred to below as a parent), can make the request on the child's behalf. Where a parent applies on behalf of a child, an authority should be satisfied that the child lacks capacity to make a valid application, or has capacity and has authorised the parent to make the application. Where the child does not have capacity, the authority also needs to be satisfied that the request made by the parent on the child's behalf is in that child's interest.

5.10 Where an authority considers that granting access to a parent is likely to result in serious harm to anyone, including the child, the authority will need to decide whether to refuse access on the grounds set out in paragraph 5.37 below. If an authority refuses to disclose data to a parent either on the grounds that the request is not in the child's interest or on the grounds that it considers that to do so would result in serious harm, that parent, acting on the child's behalf, may make an application to the Court or to the Data Protection Commissioner.
Requests made on behalf of an adult lacking mental capacity

5.11 The DPA makes no special provisions about requests for access made on behalf of an adult who lacks mental capacity and is incapable of managing their own affairs. If a person lacks capacity to manage their affairs, a person acting under an order of the Court of Protection or acting within the terms of a registered Enduring Power of Attorney can request access on her or his behalf.

5.12 Mental disorder does not equate with mental incapacity and many persons suffering from the former may have sufficient capacity to enable them to deal with their affairs. As with access by children and young persons under 18 (see above) requests for access by persons with a mental disorder will require a judgement in respect of their capacity to understand the nature of the request and the information sought.

Requests made through another person (an agent)

5.13 If a person has capacity and if she or he has appointed an agent, that person can make a valid request for access on behalf of the data subject. Agents should provide evidence of their authority and confirm their identity and relationship to the individual. Such evidence should normally be provided in writing. If an authority is satisfied that the data subject has authorised the agent to make the request, it must treat the request as if it had been made by the data subject and proceed accordingly. Access is subject to the rules specified in paragraphs 5.5-5.7 above. This also applies where a person is acting on another’s behalf, under a general power of attorney.

5.14 A person who is profoundly physically disabled may not be able to give written consent for an agent to seek access on their behalf. Where the person is unable to give written consent the local authority should give the individual as much assistance as possible. Ultimately, the authority will have to make a judgement on whether the individual has given consent for an agent to act on their behalf.

Requests for access to the records of a deceased person

5.15 The Data Protection Act applies only to data about living persons (see section 1(1)). Therefore data held on the deceased are not personal data, as defined by the Act. Even though the DPA does not apply to such data there may still be issues of confidentiality surrounding access to records about the deceased. (See section 7 below).

Dealing with a request for access, and fees

5.16 A request for access has to be made in writing (see DPA, section 7(2)(a)) and be accompanied by the appropriate fee when this is required by the authority. The fee charged must not exceed the statutory maximum of £10, including the cost of supplying copies. Authorities may provide a standard request form, but have no right to insist on its use. This could include the details necessary to identify the
subject and locate the information held, to ensure that all the information necessary to process a request for access is available at the outset. Where a person may be unable to make a written application without support, or because English is not the person's first language, authorities should make sure that suitable help is available, for example, by referring the individual to an advocacy service, the local Citizens' Advice Bureau, Children's Rights organisations or by arranging interpreters.

5.17 Where an authority has decided to charge a fee for access it should inform individuals that a fee is payable and of the amount requested. It is not required to provide the information requested or process the application until such time as the fee has been received. Responses to requests for access must be made within 40 days of the date of receipt of the request and the fee. Authorities who decide to charge a fee may take into account the applicant's ability to pay or other circumstances and decide to waive the established fee.

Where an authority does not hold the information requested

5.18 If an authority does not hold the personal information requested, it should inform the applicant as quickly as possible. An authority should not decide that there is no need to reply. The DPA makes no provision for the return of the fee paid. Where no data are discovered the authority must decide whether it should return the fee. In such cases the authority should take into consideration the situation of the data subject, the effort involved in discovering that there was no data, and the authority's policy with regard to charging for access.

Points to consider before access is given

5.19 Access can be refused where the authority has previously complied with an identical or similar request from the same individual, unless a reasonable interval has elapsed between compliance with the one and receipt of the other (section 8(3)). In deciding what amounts to a reasonable interval the following factors should be considered: the nature of the information, the purpose for which the information is processed and the frequency with which the information is altered. Also, the authority is not required to respond unless it is provided with sufficient details to enable it to locate the information and satisfy itself as to the identity of the individual making the request (section 7(3)).

Information to be disclosed

5.20 The information to be disclosed is all the data held about the data subject by the data controller (ie. the authority), unless the data are subject to any exemptions or another person has refused to consent to disclosure of data identifying them (see paragraphs 5.6 and 5.7 above). It should not be altered in order to make it acceptable to the data subject.
The information disclosed must be that held at the time the request is received. Account may be taken of any amendment or deletion made between the time of the request and the supply, if the amendment or deletion is one which would have been made regardless of the request.

An individual who makes a request for access to personal information held by an authority is entitled:

- to be told by the authority whether it or someone else acting on its behalf is processing that individual's personal information;
- if so, to be given a description of:
  - the personal information,
  - the purposes for which the information is being processed, and
  - those to whom it is or may be disclosed; (Section 7(1)(b))
- to be told, in an intelligible manner:
  - the information which constitutes the personal data,
  - the source of the information (but – see paragraph 5.6 – the authority is not obliged to disclose such information where the source of the information is, or can be identified as an individual) (section 7(1)(c));
  - where a decision significantly affecting a data subject is, or is likely to be made about them solely by fully automated means, for the purpose of evaluating matters about them such as their conduct, they are entitled to be told of the reasoning involved in that process (section 7(1)(a)).

If any other person is mentioned, and disclosure would allow her or him to be identified, an authority may decide to obtain that person's consent before disclosure. Alternatively it may decide that it is reasonable in all the circumstances to disclose without obtaining that person's consent (see section 7(4)(b), 7(6) and paragraphs 5.5 to 5.7 above).

Section 7(6) of the DPA is likely to be of particular relevance when a request is received for access to very old files and the possibility of tracing other identified persons is remote.

An authority should set itself a sensible timescale, within the 40 days allowed, in which to seek any third party consent. The 40 day period does not commence until the authority has received the written request, the appropriate fee, and if necessary, the further information required to satisfy itself as to the identity of the person making the request, and to locate the information sought.

If consent is not given by any other person whose identity would also be disclosed within 40 days, an authority should give as much information as possible without identifying that person (see section 7(5)). An authority should explain why some of the information requested has not been given. Where that
other person’s consent is not or cannot be given, and the authority considers it reasonable to comply with the request without it, it may do so. However, it may later be required to justify its actions if the person in question later says the particular disclosure was a breach of their rights under the DPA (see paragraph 5.7 above).

5.27 Where the authority is satisfied that the data subject will not be able to identify the other person from the information to be disclosed, taking into account any other information which the authority reasonably believes is likely to be in or to come in to the possession of the data subject, then the authority must provide the information.

5.28 If full access is not given or the data subject believes that the authority has failed to comply with the request he/she can apply to the Data Protection Commissioner or the courts.

Presenting the information

5.29 The DPA requires the information to be communicated in an intelligible form, and that the data subject should be provided with a permanent copy of the information (see DPA, section 7(1)c and section 8(2)). However, the authority need not supply a copy if it is not possible, or would involve disproportionate effort, or the data subject agrees otherwise, for example where the data subject wants only an extract from a lengthy file.

5.30 Some of the material to be disclosed may be known to the data subject already, but it may still be helpful to have someone available to help the data subject “take in” the material or explain anything that he or she does not understand.

Where an authority holds information the data subject considers is inaccurate

5.31 If a person considers that an authority holds personal information which is inaccurate in any way, she or he can take the following action:

- ask the data controller to correct the data;
- approach the Commissioner if he/she considers the controller has not made the requested correction;
- apply to the courts for an order requiring the data controller to rectify, block, erase or destroy the data.

The data controller maybe required to correct data judged by the DPC or courts to be inaccurate. The controller may also be required to inform other organisations who may have received the information of the correction.
5.32 The data subject may also be entitled to compensation for any damage suffered as a result of the use of data requiring rectification.

5.33 “Inaccurate” means incorrect or misleading as to any matter of fact (see section 70(2)). A mere opinion need not be corrected or erased, unless it appears to have been based on an inaccurate fact.

5.34 If an authority does not agree that the information is inaccurate, they should note in the record that the subject regards the information as inaccurate.

5.35 It is good practice for the authority to deal promptly with requests for data to be corrected in order to avoid the court action or intervention by the Commissioner which may result. The authority should also send a copy of the corrected data to the subject. Although the DPA does not set any timescale for authorities to respond to such requests, they should aim to inform data subjects of the action taken within 21 days of receiving the request.

When an authority can rely on an exemption to refuse access

5.36 Certain personal information is exempt from compliance with aspects of the non-disclosure requirements and the subject information provisions of the DPA. The purposes for which exemptions are available are described in the DPA and include information required for the purposes of social work.

5.37 Exemption from both the subject information provisions and the disclosure provisions of the DPA may be available in the following circumstances:

(i) Prevention or detection of crime: an authority need not inform the data subject –

- that it is holding personal data about him/her for the purposes of the prevention or detection of crime, or to apprehend or prosecute offenders;
- that information about him/her has been disclosed to another organisation which required it for any of these purposes (eg the Police);
- that it has received information from an organisation which had it in its possession for any of these purposes;
- that it is holding personal data about him/her if the provision of such information would be likely to prejudice disclosure or would be likely to prejudice any of these purposes (section 29).

Requests should be treated on a case by case basis and use of the exemption should be the exception rather than the rule. Legal advice should be sought where doubt exists.
(ii) The Data Protection (Subject Access Modification) (Social Work) Order 2000: this provides that personal data held for the purposes of social work are exempt from the subject access provisions, where the disclosure to the data subject would be likely to prejudice the carrying out of social work, by causing serious harm to the physical or mental health, or condition, of the data subject, or another person.

In making decisions on whether or not to give access to certain information there is no general test of what constitutes a risk of serious harm. Decisions have to be made on a case by case basis. Restriction on the right of access should be exceptional and confined to serious harm, for instance where there is sufficient risk to the safety of a child for a child protection plan to be in place and where disclosure would prejudice the plan. In some cases, access may have to be denied permanently. In others it may have to be deferred. The person seeking access may need special counselling during the period of deferment.

The Order also provides that access cannot be refused on the grounds that another person would be identified where that person is a relevant person (eg a social worker) unless the serious harm test applies. In all cases where this exemption applies the subject need only be informed that data about him are being processed. (A note describing the full extent of the Order appears as Appendix 2 to this guidance.)

(iii) The Data Protection (Subject Access Modification) (Health) Order 2000: this provides that the authority must not disclose information about physical or mental health or condition without first consulting an “appropriate health professional” (as defined in the Order). This would normally be the person responsible for the data subject’s current clinical care in connection with the matters to which the information relates. This might, for example, be a GP or psychiatrist.

(iv) The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000: where other enactments themselves prevent disclosure, then a data subject cannot rely on the DPA to seek access to records. These include, for example, adoption records and reports, and parental order records and reports under section 30 of the Human Fertilisation and Embryology Act 1990.

5.38 Local authority staff, members and officers, can use the DPA to gain access to information about themselves held in “accessible public records”, if they are also service users and the information is held for this purpose.

Where an authority decides to refuse access

5.39 Any notification of refusal to disclose personal data should be given as soon as practicable and in writing, even if the decision has also been given in person. An authority should record the reasons for its decision and explain these to the data
subject, unless there is good reason not to, for example, where reliance is made on the exemptions in Section 29 of the DPA.

5.40 If an authority decides not to disclose some or all of the personal information, the applicant must be told the reasons, distinguishing between reliance on an exemption, and failure or inability to obtain the consent of another person whose identity would be disclosed, or such a person’s refusal to consent.

Challenge to an authority’s decision to refuse access or amend records

5.41 If disclosure is refused by an authority, the data subject may appeal that refusal either to the DPC or the Courts. It is for the data subject to decide which “appeal” route to take. The Court has the power to order disclosure for example, or to order correction or erasure or to confirm non-disclosure. This right of appeal includes eligible manual data otherwise exempt during the first and second transitional periods (see section 12A, inserted by Schedule 13).

5.42 The DPC may issue enforcement notices for a breach of the Data Protection principles, but only if the Commissioner is satisfied that a contravention has taken or is taking place (see section 42). During the first transitional period only the sixth data protection principle applies to manual data where processing was already under way prior to 24th October, 1998. There are also limitations in respect of automated data where processing was already under way prior to 24th October 1998 (Schedule 8, paragraph 13).

Appeal by data controller against enforcement notices to Data Protection Tribunal

5.43 There is a right of appeal to the Data Protection Tribunal against an enforcement notice. The notice may be cancelled or varied in certain circumstances.

Conclusion

5.44 Implementation of the Act creates a single regime for access to personal information held in written or computerised records by social services departments. This should be easier to understand and operate.

5.45 It also provides the necessary avenue of appeal to an independent body about any decisions to refuse access to records. Crucially, this right can be exercised in cases where rights of access have been refused on the ground that another person who has supplied information has not consented to its disclosure, where this would identify him or her, or where that person cannot be found in order for their consent to be sought.
SECTION 6

Confidentiality of personal social services records

6.1 This Section does not apply to access by an individual to information about himself, which is dealt with in Section 5.

General Principles

6.2 Local authorities have a general duty in common law to safeguard the confidentiality of personal information which they hold in connection with their social services functions.

6.3 Where an authority wishes to disclose confidential information to another person, it will need to consider carefully whether this is lawful under the Data Protection Act 1998 (see for example the conditions referred to in paragraphs 5.6 and 5.7 of this guidance).

6.4 The DPA applies to all new processing of personal data, both in manual files and by electronic means. Until the end of the first transitional period on 23 October 2001 only the subject access provisions of the DPA apply to existing manual files held by social services departments. There are also certain exemptions for the DPA’s requirements in respect of computerised records in existence at 24 October 1998 (schedule 8, paragraph 13).
6.5 In cases of doubt, where disclosure is proposed, as to whether the DPA applies or whether only the common law of confidentiality applies, an authority should seek the advice of its lawyers. An authority should always record its reasons for deciding not to observe the duty of confidence it owes to the person who is the subject of the information.

Circumstances when personal information can be disclosed to others

Disclosure with consent

6.6 Under the DPA, where it applies fully to the data in question, then the disclosure must satisfy at least one of the conditions necessary to ensure the processing is fair and lawful, as required by the first data protection principle. These conditions are set out in Schedule 2 to the DPA. If the data is “sensitive personal data” (see glossary) one of the conditions in Schedule 3 must also be met.

6.7 Among these conditions is the requirement to have the consent, or in the case of sensitive personal data the explicit consent of the person about whom the information is held (the data subject).

6.8 Where the disclosure of the personal data is necessary in order to comply with a legal obligation imposed on an authority, then the consent of the data subject is not necessary. Authorities should, however, inform the subject that such an obligation exists.
6.9 Compliance with the conditions in Schedule 2 and Schedule 3 to the DPA is not required in the first and second transitional periods where processing (including storing) of the data in question was being carried out before 24th October 1998 (see paragraphs 4.5 to 4.9 of this guidance).

Note: The DPA does not define consent.

The EU Directive defines the data subject’s 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’.

The fact that consent has to be signified means that there must have been some communication between the authority and the subject. Failure by the data subject to reply to such a communication, for example non-return of a form requesting consent, must not be assumed by the authority to imply consent.

It may be necessary for authorities to evaluate the adequacy of any consent to ensure that it has not been obtained under duress or on the basis of misleading information.

Any consent given is only for the particular purpose or disclosure specified by the authority and must be appropriate to the circumstances specified.

The data subject may be able to withdraw consent and has a right to object to “processing”. In the case of sensitive personal data the consent where required must be explicit. In such cases the data subject’s consent must be absolutely clear and cover such items as the specific detail of the processing, the data to be processed and the purposes of the processing.

6.10 Under the common law, where the Data Protection Act does not apply, the same principles concerning disclosure with consent under the DPA apply.

Note: Much of the personal information held for social services purposes is required under statute, and in many, if not most, cases there will be no need to seek the subject’s consent to its use. However, as a matter of good practice, consent to disclosure should be sought wherever possible.

Disclosure without consent

6.11 Where the DPA applies to the data in question, disclosure without the consent of the subject is lawful where at least one of the other conditions set out in Schedule 2 to the Act is met; and, where the data is “sensitive personal data”, where one of those in Schedule 3 is met.

6.12 Relevant conditions under Schedule 2 include:

- processing necessary for compliance with any legal obligation to which the authority is subject;
- the processing is necessary for the administration of justice;
- the processing is necessary to protect the vital interests of the data subject.

6.13 The principles relating to disclosure are comparable under the common law where the Data Protection Act does not apply.
6.14 Disclosures without the consent of the person who is the subject of the information fall broadly into two groups, social services purposes and other purposes.

**Social services purposes**

6.15 An authority may disclose personal information to social services staff directly involved in a case and their line-managers. An authority may also disclose personal information to anyone else who cares for one of their clients, for example, a voluntary body or foster carers, where the information is, or is likely to be, needed for the purposes of that care. This would include any independent providers that the authority has contracted with to provide social care.

6.16 Volunteers and informal carers may also need to be given some personal information about that person. Where an individual or other organisation is providing services, on behalf of an authority, the need for confidentiality of client information should be set out in the contract between the authority and that individual or organisation.

6.17 Any disclosure of personal information should take place in accordance with established policy and procedures and, wherever possible with the consent of the subject.

6.18 Other departments of the authority, and other organisations, may also need personal information to enable the authority to discharge its statutory functions. These include for example:

- health, education
- child protection
- inspection/audit
- legal advisers
- local authority finance staff
- police

6.19 An authority may need to disclose personal information to senior managers responsible for quality assurance and service planning. Usually, only aggregate or anonymised information will be needed. But from time to time, an authority will need to disclose identifiable personal information to a senior manager, for example where a formal complaint has been made against the authority or a claim for compensation made.

6.20 An authority may need to disclose records to social services students and trainees and arrange for them to have some contact with clients, so that students and trainees are able to gain practical experience.

6.21 The local authority must ensure that anyone who is given access to personal information is made aware of the need to treat the information as confidential, and should be aware of and can be given copies of this guidance.

**Disclosure for other purposes**

6.22 An authority will need to disclose personal information to various bodies, with
the power to order disclosure, when ordered to do so. Professional and legal advice should be sought and considered in each case. Any information disclosed should be the minimum necessary to meet the requirements of the situation. Where such a disclosure is made, authority should record its reasons. Particular requirements of this kind include disclosure to:

• police
• the courts
• certain tribunals
• statutory inquiries
• individuals with the power to require information relevant to matters within their jurisdiction to be disclosed (the Secretary of State for Health, the Commissioner for Local Administration, Guardians ad litem and reporting officers, the Health and Safety Executive, etc).

Disclosure of information about those without capacity to consent

6.23 The same rules about disclosure of information apply to all those who are too young to understand, or to adults who lack capacity and are incapable of managing their own affairs. Where appropriate, consent should be obtained from the person with legal authority to act on the person's behalf (see paragraphs 5.8 to 5.12). In other cases, public interest arguments apply to the breach of confidence.

Sharing information

6.24 Clear procedures for sharing information should be adopted formally within authorities, subject to necessary legal advice and consultation with staff representatives. The procedures should be kept under review.

6.25 A statement of the authority's policies and procedures on confidentiality and the disclosure of information should be available and publicised. This will help to ensure that data subjects and providers of information are aware of how and why records will be kept and shared. It may be necessary in some circumstances, however, to obtain specific consent to disclosure. Attention should always be paid to the safeguards necessary to protect a service user where information has been provided by another person.

6.26 Procedures for disclosure should be simple and unambiguous and specify:

• post holders who are to deal with requests for disclosure;
• procedure to be followed and time limits operating
• safeguards to ensure that information will only be used for the purpose for which it was obtained.

6.27 There are cases where it may be necessary to disclose all of the contents of a record to another authority or organisation. Generally, however, it will be more
appropriate and sufficient to make available that which is relevant for the purpose for which it is required. Disclosure may be made in the following ways:

- in writing;
- by provision of a copy;
- orally;
- electronically, from one computer to another.

6.28 Care is necessary when making oral disclosure that conversations cannot be overheard and that individuals to whom personal information is disclosed are aware of the confidentiality implications of such disclosure. Use of the telephone as a means of disclosing information, especially confidential information, should be avoided where possible. A record of all oral exchanges of information should be kept and confirmed in writing.

Disclosure of Information for research purposes

6.29 The DPA provides exemption from the subject information provisions and disclosure requirements for data required for research purposes. Such data must not be processed to support measures or decisions with respect to particular individuals or in a way that could result in substantial damage or substantial distress to the data subject. The results of the research must not, moreover, be made available in a form which identifies any data subject or subjects.

6.30 Before disclosing data for research purposes the authority must ensure that:

- where an individual subject has objected to the use of personal data about him/her that such data are not disclosed to the researchers
- research workers undertake to comply with the authority's policy and procedures
- research workers do not approach data subjects without the authority's consent
- the data will not be disclosed to third parties not involved in the research
- the results of the research will not identify or enable any individual to be identified
- the data used for the research will be kept secure and that all data no longer required for research will be destroyed within an agreed time scale.

Monitoring

6.31 It is important to maintain public confidence in the confidentiality of information held by the authority. A record of exceptional disclosures should be maintained, and reviews, with statistics, of the number and nature of disclosures within the excepted categories should be made available for publication from time to time. Local authorities should also monitor requests for access, in order to ensure that they are complying with the requirements of the DPA.
APPENDIX 1

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in a manner incompatible with that purpose or those purposes.

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

4. Personal data shall be accurate and, wherever necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than it is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

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

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the procession of personal data.

[See schedule 1 of the DPA]
APPENDIX 2

THE DATA PROTECTION
(SUBJECT ACCESS MODIFICATION)
(SOCIAL WORK) ORDER 2000

1. The Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI 2000/415) provides for the partial exemption from the provisions of the DPA of the rights of subjects to gain access to data held about them, where the exercise of those rights would be likely to prejudice the carrying out of social work, by causing serious harm to the physical or mental health or condition of the data subject or another person.

2. The Order does not apply to any data to which the Data Protection (Subject Access Modification) (Health) Order 2000 (S.I. 2000/413), the Data Protection (Subject Access Modification) (Education) Order 2000 (S.I. 2000/414) or the Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (S.I. 2000/419) or any order made under section 38(1) of the Act applies (article 3(2)).

3. Broadly, the Order confers an exemption from section 7(1)(b) to (d) of the Act, leaving only the right of the data subject to be informed by any data controller whether data about him are being processed by or on behalf of that data controller.

“Relevant persons”

4. The Order also modifies section 7 of the Act, so that a data controller cannot refuse access on the grounds that the identity of another person would be disclosed in cases where that other person is a “relevant person”, unless serious harm to that person’s physical or mental health or condition is likely to be caused by giving access, with the result that the exemption in Article 5(1) applies.

5. The term “relevant person” is defined in the Order, and includes anyone who:

(a) is employed by a person or body within the scope of the Order, such as a local authority social worker, or
(b) has performed for reward a service similar to a service provided by a local authority, such as foster parents or informal carers who receive a payment from social services for caring for another person (but not informal carers who are unpaid).

6. A further exemption from the subject access provisions is conferred in certain circumstances where another person is making the request for access on behalf of the data subject and the data subject does not wish that information to be disclosed to that person.

7. There are also rights of appeal to the court, both for a person who has been refused access and for any person who considers that if access is given this may lead to serious harm being caused to him or her.
APPENDIX 3
DATA PROTECTION
ADVISORY GROUP

Trish Davies  
Social Care Group,  
Department of Health

John Cypher  
Social Services Inspectorate

Dick Beaver  
Social Services Inspectorate

Sue Ryan  
Solicitors,  
Department of Health

Paul Woods  
Social Care Group,  
Department of Health

Alan Chapman  
Local Government Association

Michael Hake  
ADSS

Nick Bishop  
Royal Borough of  
Kingston-Upon-Thames

Paul Ainsworth  
Cambridgeshire County Council

Phil Wareham  
Milton Keynes County Council

Penny Prior  
Northamptonshire County Council

Richard Humphries  
Herefordshire County Council

Nick Tomlinson  
Bournemouth Borough Council

Ian Robertson  
Consultant*

David Truan  
NSPCC

Stuart Bond  
Scottish Office

Colin Vvyyan  
Welsh Office

* Assisted in the drafting of the guidance