

**Access to Records  
Policy and Procedures  
(for Service Users)**

---

---

**July 2005**

## **Foreword**

The contents of this document are for staff to use when responding to formal requests from service users for access to their personal records compiled and held by Slough Borough Council (SBC) as part of its social services responsibilities.

Access to service users records by others e.g. researchers, inspectors, elected members, social work or other students in training, is not included and staff should make reference to other internal and external documents. E.g. SBC Corporate guidance on the Data Protection Act and on the Freedom of Information Act. Also the Data Protection Act 1998 and associated Guidance to Social Services, Department of Health (March 2000); the Freedom of Information Act 2000; and Department of Health guidance on 'Caldicott' Guardians relating to 'Patient-Identifiable Information'.

Staff are reminded that they should consult the primary sources of information on protecting data and access to records, namely the Data Protection Act 1998 itself, as well as the Department of Health guidance referred to above, and not rely solely on this document.

Staff should also ensure that they consult a sufficiently senior line manager e.g. Service Manager or Head of Service or the SBC 'Caldicott' Guardian, as well as taking necessary legal advice, particularly where issues of disclosure are concerned e.g. those matters where consent is sought or where disclosure is withheld or where disclosure is being considered without consent.

## INDEX

	Page
1. Purpose	1
2. Scope	1
3. Legislation	2
4. Policy and Principles	2
5. Rights of Access (who can have access?)	3
5.4 Access by a child/young person	3
5.5 Requests made on behalf of a person lacking mental capacity	4
5.6 Request through an agent	4
5.7 Requests for access to the records of a deceased person	5
6. What Information is Available for Access	5
6.5 Records held in joint teams	5
6.6 Implications of the Data Protection Act 1998 and its implementation	6
7. Exemptions	7
7.2 Risk of serious harm	7
7.3 Prevention of a crime	7
7.4 Information about physical or mental health or condition	7
7.5 Legal professional privilege	8
7.6 Adoption records and other enactments	8
8. Responding to Formal Requests for Access	8
9. Preparing Records for Access	9
10. Establishing the Identity of the Applicant (or their agent)	11
11. Preparing for Access and Viewing of the Records	11
11.9 Correction or erasure	12
Appendix A Data Protection Principles and ‘Caldicott’ Principles	
Appendix B Glossary	
Appendix C Standard letter to third party – Health Professional / Manager of Agency requesting consent to give access to information	
Appendix D Letter of acknowledgement/explanation to applicant requesting access to records	
Appendix E Access to Records progress Log Form	

# **Social Services Access to Records (Service Users) Policy and Procedures**

## **1 Purpose**

- 1.1 To provide a framework and guidance for staff when responding to requests from service users for access to records about themselves compiled and held by Slough Borough Council (SBC) when carrying out its Social Services responsibilities.
- 1.2 To enable staff to deal consistently with such requests and so that access arrangements comply with all legal requirements associated with accessing personal data.

## **2 Scope**

- 2.1 This document covers arrangements for dealing with formal requests for access to personal records held by SBC when fulfilling its social services responsibilities, whether held electronically, or in 'relevant filing systems' or in 'accessible public records'. In other words, any information held about a particular individual by SBC for the purpose of this authority's social services functions, irrespective of when the information was recorded. (for definitions see Glossary, Appendix B)
- 2.2 This policy applies to personal information held on service users and not personal information held on employees of SBC. (Employees will need to refer to Corporate personnel managers for guidance on access to their records)
- 2.3 Records containing personal information may be held in different locations or by different teams and for the purposes of this guidance all such information is potentially discloseable to the subject or their authorised agent.
- 2.3 A personal record will include any personal data (information) where ever held and will include computer held information, manual files held in units, day books, card indexes, financial records, residential, day or domiciliary care records.

### **3. Legislation**

3.1 The statutory framework relevant to this document includes:-

- The Data Protection Act 1998 (DPA)
- Data Protection Act 1998: Guidance to Social Services (March 2000)
- Crime and Disorder Act 1998
- Judgement of the European Court of Human Rights 1989 (Gaskin vs UK)
- Human Rights Act 1998 ( in force from October 2000)
- Freedom of Information Act 2000 (FOI) (In force 2005)
- Mental Capacity Act 2005 (to be implemented in 2007)

3.2 This document relates to other social services and corporate policies on:-

- Records Retention and Destruction Handbook (2005)
- Case Recording – Policy, Principles and Procedures (2005)
- Data Protection
- Freedom of Information

### **4. Policy and Principles**

4.1 Under the Data Protection Act 1998, any living person has a right of access to personal data about themselves. Where access is refused, the individual (data subject) may appeal to the courts or the Data Protection Commissioner.

4.2 Social services will inform service users when information is held about them and of their right of access. (Note See SBC Corporate information leaflet - "Personal Information: Your Right to Know")

4.3 Social services has an open access policy of allowing and encouraging service users to have free informal access to personal information held about them, subject to certain exemptions.

4.4 Social services have a policy of regarding record keeping and access to records as part of the service to service users. Central to this policy is adherence to the principle that it is good social work practice for workers to maintain open professional relationships with service users, to share judgements, to plan together and to check information. This participation and openness includes service users contributing to the compiling of their records and their involvement in agreeing care plans.

4.5 Formal access to closed records will be provided free of charge.

- 4.6 Assistance will be offered to service users or their authorised agents so that access can be gained for individuals who may have difficulties as a result of any disability or impairment. Staff will also be available to assist in 'going through' a service users record so that they can better understand what is recorded and available to them.

## **5. Rights of Access (who can have access?)**

- 5.1 Access to personal data will normally be given only to the data subject. Any user of services and any other living person about whom social services hold personal information in connection with its social services functions has the right of access to personal information about themselves. This includes foster carers, childminders, Persons registered under National Care Standards requirements and other carers (such as supported lodging carers) who are not employees of the local authority.
- 5.2 An individual is not entitled to know what is recorded about another individual with out consent.
- 5.3 Individuals can apply for access to their personal records through an agent or representative.

### **5.4 Access by a child/young person**

- 5.4.1 Those under the age of eighteen have a right of access to their records if the child making the request is considered to understand the nature of the request. There is no minimum age requirement.
- 5.4.2 The social services officer responsible for over seeing the process and progress of the request for access (the 'Responsible Officer'), must decide whether or not the child has sufficient understanding to make the request for access. That is, does he or she understand the nature of the request? If so, then the request for access should be complied with.
- 5.4.3 If a child does not have sufficient understanding to make his or her own request, a person with parental responsibility (referred to below as the parent) can make the request on the child's behalf.
- 5.4.4 Where a parent applies on behalf of a child. the responsible officer 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 Responsible Officer needs to be satisfied that the request made by the parent on the child's behalf is in that child's interest.

- 5.4.5 Where the Responsible Officer considers that granting access to a parent is likely to result in serious harm to anyone, including the child, the officer will need to decide whether to refuse access on the grounds set out in section 7 (exemptions). Where the decision not to disclose data to a parent either on the grounds that serious harm may result, that parent, acting on the child's behalf may apply to the Court or Data Protection Commissioner for access.
- 5.4.6 The Responsible Officer should obtain legal advice from SBC's legal team, where necessary, when considering not to allow access to a child's record by a parent. The reasons for refusing to allow access should be given to the applicant, as soon as practicable and in writing, even if the decision has already been given in person. The reasons for the decision made must be recorded on the individual's file..

## **5.5 Requests made on behalf of a person lacking mental capacity**

- 5.5.1 If a person with a mental disorder has legal capacity, i.e. she or he understands the nature of the request, she or he can request access. The DPA makes no special provisions about requests made on behalf of an adult who lacks mental capacity and is incapable of managing their 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 or a Guardian under the terms of the Mental Health Act 1983, can request access on his or her behalf.
- 5.5.2 Mental disorder does not, of itself, equate with mental incapacity. Where there is doubt about an individual's capacity, consideration should be given to obtaining medical advice, in the form of a psychological or psychiatric assessment in order to gauge whether an individual has the capacity to make a request in their own right.
- 5.5.3 The Mental Capacity Act 2005 will be implemented in 2007. One of the underlying principles of this Act is a presumption of capacity unless it is proved otherwise. Also under the Act an individual must be given all appropriate help before it can be concluded that he or she lacks capacity. A Code of Practice will be published to accompany the Act and when this is available its contents should be followed.

## **5.6 Request through an agent**

- 5.6.1 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. If the local 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

5.6.2 A person who is profoundly physically disabled may not be able to give written consent for an agent to apply for access on their behalf. Where a person is unable to give written consent, staff should give the individual as much help as possible and will need to make a judgement on whether the individual has given consent for an agent to act on their behalf.

## **5.7 Requests for access to the records of a deceased person**

The DPA applies only to data about people who are alive. Personal data held about someone who has died may, at the Responsible Officer's discretion, (in consultation with SBC's Corporate Data Protection Officer and/or 'SBC's 'Caldicott' Guardian and/or SBC's legal team), be disclosed to others who have a sufficient interest in the matters recorded.

## **6. What Information is Available for Access**

6.1 Accessible information is any information held by social services on an individual that is held in "accessible public records" as part of a local authority's social services function conferred by virtue of the Local Authority Social Services Act 1970.

6.2 The information held will include that held on computer, in files, microfiches, card indexes, day books, material prepared and held for any legal proceedings. It will include letters, reports, records of direct contact and telephone calls, records of meetings and case conferences.

6.3 This information may be held in Town Hall offices, residential homes, day centres and held by staff employed by social services in any out-posted teams.

6.4 Where a service is being provided by another organisation on behalf of the local authority, a request for access to information arising out of that service should be made to that other organisation.

### **6.5 Records held in Joint Teams**

6.5.1 Where there are services provided in partnership between social services and another organisations e.g. NHS trust, an application for access to records will need to be responded to in the following way:-

- Where “joint records” are held in joint teams where staff contribute to the same record on an individual, the individual should not have to apply to both organisations for access to their records.
- The term “joint record” as used above does not include records held separately by social services 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, these are not considered “joint records”. In this case individuals would need to make application to both organisations.

## **6.6 Implications of the Data Protection Act 1998 and its implementation**

6.6.1 The Data Protection Act 1998 (DPA) is being implemented in stages and applies to social services records as follows:-

6.6.2 Already implemented:- Access to Records - applications made between 1st March 2000 and 23 October 2001:-

- For records made (data processed) on or after 24<sup>th</sup> October 1998 all provisions of the Data Protection Act 1998 will apply

6.6.3 For records made before 24<sup>th</sup> October 1998 access requests will be made under the DPA and the following conditions apply:-

- Applicants will not have a right under the act to rectify the content of their record, for compensation for errors made or to apply to the Court or to the Data Protection Commissioner where the disclosure of information from sources other than the data subject is withheld.

6.6.4 The second transitional stage is from 24<sup>th</sup> October 2001 to 23<sup>rd</sup> October 2007 and applies to certain manual data held in social services records immediately before 24<sup>th</sup> October 1998.

6.6.5 After 24<sup>th</sup> October 2007 all parts of the Data Protection Act will apply, whenever the records were made.

6.6.6 It is the policy of SBC to work in partnership with services users, where ever possible and that case recording is part of the service the council provides. It is the intention of staff, whilst exercising the council’s social services responsibilities, to share as much information as possible with service users and will work in a way that anticipates the provisions of the Data Protection Act 1998 and access to records arrangements so that the fullest co-operation can be achieved. This includes correcting inaccuracies and that the council will be seek consent from sources other than the data subject, to disclose information and may disclose information without consent where they consider this appropriate.

## **7 Exemptions**

7.1 Providing access to and disclosing certain kinds of personal information held in social services records is exempt from the provisions of the DPA. The following are examples where information may not be disclosed:-

### **7.2 Risk of serious harm**

7.2.1 Access to personal information may be refused where the performance of the authority's functions would otherwise be prejudiced because access is thought likely to result in serious harm to the individual's physical or mental health or that of some other person.

7.2.2 Staff need to bear in mind that the fundamental principle is that individuals should be able to see what is recorded about them and it is for this reason that this limitation is restricted to serious harm. Withholding information on this ground is therefore likely to be exceptional. The council may only withhold just so much of the information as is likely to cause serious harm, or enable the identity of another to be disclosed or deduced.

### **7.3 Prevention of a crime**

7.3.1 The council need not disclose information which is held for the purposes of the prevention or detection of crime, or to apprehend or prosecute offenders if disclosure would be likely to prejudice one of these purposes.

### **7.4 Information about physical or mental health or condition**

7.4.1 Information supplied by a "Health Professional" should not be disclosed without seeking consent from the supplier of personal medical information about an individual. This would normally be the person responsible for the individual's current clinical care in connection with matters to which the information relates.

7.4.2 When writing to a health professional or other third party source, about information supplied and held on social services records, advice about the time scale for response should be given and that if a response is not received within the period access may be provided to the individual. (Appendix C)

7.4.3 Where additional health information or explanation about that information is required individuals should be advised to discuss the matter with the appropriate health professional (For definition of A Health Professional see glossary Appendix B)

## **7.5 Legal professional privilege**

7.5.1 Personal information is exempt from access if it consists of information where a claim for legal professional privilege could be maintained in legal proceedings. Legal advice obtained by social services about a data subject should be held in the confidential section of the case record.

## **7.6 Adoption records and other enactments**

7.6.1 Where other enactments themselves prevent disclosure, then the data subject cannot rely on the DPA to seek access to records. These include adoption records and reports; parental order records and reports.

7.6.2 Any requests for access to Guardian ad Litem records should be directed to the GALRO panel manager as the information held in these records is not held for the purposes of a social services function.

7.6.3 Where a social work record holds information prepared for care proceedings, the child or parent can have access to these if they were party to the proceedings. Any other person, apart from a solicitor or counsel appointed by the child or parent, must seek leave of the court. Similar rules apply to papers prepared for Wardship Proceedings.

## **8. Responding to Formal Requests for Access**

8.1 The social services Case Recording Policy, Principles and Procedures (2005) sets out expectations and requirements for case recording, emphasising partnership, sharing and openness and that case recording is part of the service to service users.

8.2 Case records generated in recent times and from now on will have much of the content already known to the individual to whom the record relates. This has not always been the case and it has only been since 1987 – The Access to Personal Files Act - that rights have been established for individuals to request access to their social services records.

8.3 A request for formal access must be made in writing and in the first instance will be addressed to the Corporate Data Protection Officer. A written request for access does not have to be on the prescribed form in order to be valid.

8.4 A letter acknowledging receipt of the request (Appendix E) should be sent within 24 hours of the request being received. The request and acknowledgement letter will then be passed to the appropriate team

manager / Access to Records Officer ( the 'Responsible Officer') who will oversee the process and co-ordinate the response, as well as guide the worker designated to undertake the detailed work involved. (A copy of the application and acknowledgement letter should be sent to the appropriate officer so that all formal requests for access can be properly logged and monitored).

- 8.5 At the earliest opportunity steps should be taken to clarify with the applicant the precise nature of the information they seek, if this is not clear from the completed application form. Applicants may wish for a single piece of information, which can easily be given, in which case they may not wish for full access, although they retain the right for this.
- 8.6 Access to the record must be provided within 40 days of receiving a request. Where there is likely to be a delay in making the record available, because of matters relating the third party consents for example, the applicant should be informed. Their agreement should be obtained if the 40 day period is likely to be exceeded in order to prepare the record fully. However, the Responsible Officer must work towards making available as much of the record as possible within the 40 day period.
- 8.6 A request for access might be made for a record that is current, where a service is being provided, a record where services are no longer provided and the record has been 'closed' within the last five years, or a record that has been 'archived'. Records held in the archived system may consist of manual files , microfiched records or only consist of brief details on a card index.
- 8.7 The applicant should be advised of the processes involved, obtaining third party consents, getting information together (if likely to be in a number of different locations), what information is and what is not accessible and including the time scales.
- 8.8 The worker who is directly dealing with the request should complete the Access to Records Progress Log form ( See Appendix F.) which will be attached to the file(s) and completed throughout the process.

## **9. Preparing Records for Access**

- 9.1 Having established with the applicant the nature of the information they are seeking, the worker will need to assemble the appropriate records (from all locations) and ensure that the content is in order. This will involve ensuring that any of the contents of the record(s) have been checked so that only appropriate information is accessible.

- 9.2 Personal information held on a service user's record may include details about another person. If disclosure would allow her or him to be identified, the Responsible Officer, or delegated worker should make every effort to obtain the other person's consent before disclosure; or the Responsible Officer may decide that it is reasonable, in all the circumstances, to disclose without obtaining such consent. (Note The GALRO home address should not be on the file. The GAL panel address should be used instead. Individual police officers should not be identified by name but referred to as The Police Authority if this is the source of the information).
- 9.3 To decide what is reasonable, the following factors must be considered:-
- Any duty of confidentiality owed to the third party
  - Any steps taken to seek their consent (see Appendix C)
  - Whether the third party is capable of giving consent
  - Whether consent has been expressly refused.
  - Any legal prohibition.
- 9.4 Where a record contains personal information supplied by a third party (other than a health professional) steps should be taken to obtain their consent to disclose this information to the data subject. (Appendix G)
- 9.5 If consent is not received from a third party within 40 days, the local authority should give as much information as possible without identifying the third party and should give an explanation why some of the information requested has not been given.
- 9.6 Sometimes it will be clear that the information can be given without the other person's consent, e.g. where the service user has given the information about the other person in the first place.
- 9.7 When 'editing' information to not reveal an other person's identity or to prevent it being deduced, only the minimum amount of alteration for this purpose should be made e.g. "Ms. Nazine Joshi reported to us..." should be amended to "X reported to us....". Where this kind of editing is required extreme care should be taken to ensure the original entry cannot be recognised.
- 9.8 These kind of amendments referred to in para 9.7 above are acceptable within the DPA guidance providing there are no other special amendments that otherwise would not have been made. As far as possible the personal information revealed to the data subject should be that contained in their record at the time the request for access was received. Routine amendments as outlined above are acceptable but the information must not be tampered with to make it more acceptable to the individual.

9.9 Where the Responsible Officer is unclear about the necessity for third party consent to disclose or any other matters about revealing or withholding information, advice should be sought from their line manager and if appropriate, legal advice obtained.

## **10 Establishing the Identity of the Applicant (or their Agent)**

10.1 Where the worker directly involved in arranging access to the record does not know the applicant or their agent, proof of identity must be requested before any personal information is revealed. A copy of a birth certificate, passport or other clear proof of identity should be placed on the file as confirmation.

10.2 Where an individual will not be present when their agent is being provided with access, they will be advised in advance, that their agent will need to produce proof of identity.

10.3 If the applicant (or their agent) fails to provide information confirming their identity then the Responsible Officer will write to inform her/him that their request to access the personal record cannot proceed.

## **11. Preparing for Access and Viewing of the Records**

11.1 Having established from the applicant the nature of the information they seek the worker will have ensured that the records are prepared in the following way by:-

- Removing material where exemptions apply (see paras 7.1 to 7.6)
- Removing names and information given by third parties. (see paras 9.7 & 9.8)
- Photocopying the records

11.2 When all the available material has been checked by the Responsible Officer, a date and venue should be arranged with the applicant (or their agent) within the required time scale. That is 40 days from the date of receipt of the formal request for access and when the Responsible Officer has ensured that the applicant or their agent have been properly identified and or their authority confirmed.

11.3 The worker will need to ensure that the venue is a suitable one having regard to any special needs the applicant may have.

11.4 The worker will need to ensure identity is established and in the case of an agent that they have given a written undertaking not to disclose the information provided to anyone other than the person on whose behalf she/he is acting, without that person's consent.

- 11.5 The worker should remind the applicant of what information will and will not be available to them and why (e.g Information from other sources)
- 11.6 The worker will also need to assess the impact on the individual of any personal information they receive from their record(s) and report to the Responsible Officer where further assistance/counselling may be required.
- 11.7 The worker should note any claims of inaccuracies in the records and explain how these will be dealt with and refer to the responsible officer.
- 11.8 The records should be made available at council premises (i.e. the local office) unless another suitable and appropriate alternative is necessary. Photocopying facilities need to be available to supply copies of the record if requested by the applicant.

### **11.9 Correction or erasure**

- 11.9.1 If an individual considers that any personal information held on their record is inaccurate they may apply in writing for it to be corrected or erased, supplying any written material they consider supports their view.
- 11.9.2 Inaccurate means incorrect or misleading about any matter of fact. An opinion which does not purport to be a statement of fact, cannot be challenged on the grounds of inaccuracy. Inaccurate personal information can be erased or corrected whether received from the individual or from a third party. If the social services worker does not agree to the request to correct or erase any personal information a note should be included on the record that there is not agreement on this matter. The worker should consult the Responsible Officer for guidance.
- 11.9.3 The worker should be present at all times when access is taking place and ensure that the record is not removed or tampered with in any way. Under no circumstances should the individual (or their agent) take possession of the record.
- 11.9.4 In certain circumstances it may not be possible to view the available record(s) in one 'sitting' and a subsequent viewing required. The worker should ensure that at the end of the access session(s) a written statement, to go on the record, is prepared and agreed with the individual about what has been decided and any further/future actions.

SBCAccessstoRecordsPolDoc06.05

### The Data Protection Principles

- 1a Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the following conditions are met:
- with consent
  - to perform a contract with the individual
  - under a legal obligation
  - to protect the vital interests of the individual
  - to carry out public functions
  - to pursue the legitimate interests of the business unless prejudicial to the interests of the individual
- 1b Sensitive personal data shall not be processed unless at least one of the following conditions are met:
- with explicit consent
  - under a legal obligation in the context of employment
  - to protect the vital interests of the individual where consent cannot be given or is withheld
  - by certain non-profit bodies about their members
  - where the information has been made public
  - in legal proceedings
  - to carry out certain public functions
  - for medical purposes
  - is necessary for the purpose of identifying the existence or absence of equality of opportunity
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 is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the right of data subjects under this Act (DPA)
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 the possession of personal data.

(See schedule 1 of the Data Protection Act 1998)

**Caldicott Standards – General Principles**

**Principle 1 - Justify the purpose(s)**

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

**Principle 2 - Do not use personally identifiable information unless it is absolutely necessary**

Personally identifiable information items should not be used unless there is no alternative.

**Principle 3 - Use the minimum necessary personally identifiable information**

Where use of personal identifiable information is considered to be essential, each individual item of information should be justified with the aim of minimising the need to identify individuals.

**Principle 4 - Access to personally identifiable information should be on a strict need-to-know basis**

Only those individuals who need access to personally identifiable information should have access to it, and they should only have access to the information items they need to see.

**Principle 5 - Everyone should be aware of their responsibilities**

Actions should be taken to ensure that those handling personally identifiable information – both practitioner and non-practitioner staff – are aware of their responsibilities and obligations to respect an individual's confidentiality.

## **Glossary**

### **Accessible record**

Includes health records and accessible public records.

### **Accessible public record**

Means any record which is kept by a Council with Social Services and is a record of information held for any purpose of the authority's social services functions.

### **Agent**

Means a person authorised expressly by the data subject to act on his or her behalf

### **Caldicott Guardian**

Caldicott Guardians are senior staff in the NHS and Social Services appointed to protect the personal information of service users. They were introduced following the Caldicott Review of Patient-Identifiable Information (1997), which recommended that 'Guardians' of patient information should be created to safeguard and govern the uses made of confidential patient information within NHS settings. The Caldicott principles were subsequently adopted by local authorities.

### **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 forms part of the accessible record.

### **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.

### **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.

### **Data subject**

Means an individual who is the subject of personal data.

## **DPA**

Means the Data Protection Act 1998

## **Health professional**

Means;

- a) a registered medical Practitioner
- b) a registered dentist as defined by section 53(1) of the dentist 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 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 any such body as a head of department.

## **Personal data**

Means data which relate to a living individual who can be identified:

- a) from those data
- 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 or opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

## **Sensitive personal data**

Means personal data consisting of information as to –

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

## **Third party**

In relation to personal data, means any person other than

- a) the data subject
- b) the data controller
- c) any data processor or other person authorised to process data for the data controller or processor.

**Slough Borough Council**

**APPENDIX C  
Social Services**

**Standard Letter to Third Party - Health Professionals or Manager of  
Agency – Requesting Consent to give Access to Information**

**CONFIDENTIAL**

Dear. (Name of Health Professional, Manager of Trust or Health Authority)

**Data Protection Act 1998 – Access to Personal Files**

**Name of Applicant.....DoB.....**  
**Address of Applicant.....**  
.....

We have received a request from the above-named person to have access to his/her records held by Social Services. As you/your agency have contributed to these records we are obliged to request your permission for the applicant to have access to any information you have provided to us by way of contacts, letters, reports etc.

Would you please advise as to whether you consider that any information we hold should be withheld or deleted, particularly if you consider that all or part of the information should be withheld  
Because of the risk of serious harm to the individual or another person

Would you please complete the response form and return it to me within 15 working days if possible, so that we are able to maintain the strict time limits involved.

Yours sincerely,

Corporate Data Protection Officer / Access to Records Officer

Enclosure

**Access to Records Request**

**Name of Applicant -**

**I give/ I do not give\*** my permission for the applicant named above to be given access to information provided by me/this agency held on Social Services Records.

**I do/do not\* consider** that access to this information will cause serious harm to the applicant or another person

\*delete as appropriate

Name.....Agency.....

Signature.....Date.....

**Documents for which third party release is being sought**

**A copy of each of the above documents is enclosed. Please either return them with this completed response form or destroy them and confirm that this has been done.**

**Letter of Acknowledgement/Explanation to Applicant Requesting Access to Records.**

Dear (Name of Applicant)

**Re Access to Personal Records  
Data Protection Act 1998**

You have requested access to any personal information held about by Slough Borough Council Social Services. This letter acknowledges receipt of your application which was received on (date).....

We may need further information from you, either to identify you if we do not now know you personally, or to help us locate any files or records that may be held.

There may be information in your records about other people, e.g. members of your family, or provided by other people e.g. from other agencies outside Social Services and we will need to seek the consent of the person giving the information, or any person mentioned in your records. We will need to write to these other people requesting their consent.

The Act allows us 40 days to make the information ready for you. It may sometimes take longer where we need to obtain consent to disclose information required about you which has been supplied by other people, but we will contact you in any event within the 40 days to disclose as much information as possible at this time.

We will contact you to arrange a suitable date and place for access. You may wish to bring someone with you so please let us know. A member of staff will be with you to help you go through your record and answer any questions you might have. You will not be able to remove any documents from the record, but you will be able to have copies if you wish.

There may be information on your record that we are not able to show you under the Data Protection Act Regulations and we will advise you as soon as possible if that is the case. Information that may not be available to you includes records relating to adoption, information from our solicitors, some information relating to criminal matters and information that may cause serious harm to you or someone else.

When you see your record if there is information on it that you feel is wrong you may ask for it to be changed and we will consider this. It will either be changed or you can add something to your record explaining why you feel it is wrong or we will record your views on the file.

If you wish to discuss any matters relating to this request for access before we contact you again please contact us. It is our intention to show you as much information as possible within the legal boundaries and to help you with your application in any way we can.

Yours sincerely

Corporate/Data Protection Officer/Access to Records Officer

**APPENDIX E**

**Access to Records Progress Log**

Responsible Officer.....

	<b>Stage/Action</b>	<b>Remarks</b>	<b>Date</b>	<b>Signature</b>
1	Written request for access received			
2	Request acknowledged	Within 24 hours letter sent (Appendix D)		
3	Date allocated to worker	Within 7 days		
4	Additional information requested to confirm identity of individual	As soon as practicable, within 40 days of item 2 above Date received —————⇒		
5	Applicant requested for further information to locate records	As soon as practicable, within 40 days of item 2 above Date received —————⇒		
6	Consent of third parties requested (to share information)	Within 21days of 2, or 4 or 5		
7	Responses from third parties received			
8	File(s) prepared for access			
9	Applicant invited to see information			
10	Applicant given access to records			
11	Names of people present at access			
12	If data subject not present, date when agent authorisation received from data subject			

	<b>Stage/Action</b>	<b>Remarks</b>	<b>Date</b>	<b>Signature</b>
13	If no data subject authorisation received date agreed that agent should act on their behalf Authorisation by _____⇒			
14	Were copies of the record requested by the applicant, if so what was provided? _____⇒			
15	Did the applicant request any correction or erasure of the record?	If yes refer to Responsible Officer and agree note to be added to record		
16	Did the applicant object to the withholding of any information?	Advise applicant (or agent) of options open to them if they wish to make matters further. See 17 below.		
17	Did the applicant wish to appeal against the decision to withhold any information?	It is for the data subject to decide which option they wish to pursue i.e. whether to appeal to the Data Protection Commissioner or The Courts		
18	Other Actions to be listed below			

Where there are any deviations from the time scales above? Please set out reasons.....

.....

.....

.....

.....

.....

**Access to Records – Record of Third Party Consents**

Name of Third Party	Address	Status	Date letter sent Requesting Consent to Disclosure	Description of any follow-up action/ decisions made if reply not received and date	Date reply received	Consent Given or Consent Withheld

**Include reasons here where the decision is made to disclose information where consents are not agreed or have not been received or cannot be obtained, stating which documents/information and by whom the decision has been made.**

Signed (Worker).....Date.....  
 Signed (Responsible Officer).....Date.....

**Record of Exemption to Access**

Where the record has been prepared for access please list below the material removed or deleted giving your reasons for this.

Material affected :-	Reasons :-
----------------------	------------

Signed(Worker).....Date.....

Signed (Responsible Officer).....Date.....

**Denial of Access**

When access to the records has been denied please give reasons :-

--

Signed (Worker).....Date.....

Signed (Responsible Officer).....Date.....

Date Access Process Completed to Satisfaction of Applicant .....
Signature (Worker).....Signature (Responsible Officer).....