Policy

Adults & Children Directorate

Subject Access Policy
(Data Protection Act 1998)

west sussex county council

Effective from: 13.12.06
Version: 4
Revised: Nov 2010
Review date: Nov 2012

Glossary of terms

Data Controller
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 is, or is to be, processed. **The Data Controller is West Sussex County Council (of which schools are not included in this case).**

Data Subject
An individual who is the subject of personal data.

Guidance "Why we have to do it"
This can be issued by government or can be a local directive on good practice. Guidance can be very specific or a more general statement of principles.

Legislation "the Law"
Issued by central government following a process of wider consultation with targeted stakeholders about the proposals (green paper), followed by a white paper detailing proposed legislation for further consultation, and then a bill which is progressed through Parliament to become law (an Act of Parliament).

Personal Data
Data which relates to a living individual who can be identified-
(a) from that data, or
(b) from that data and other information which is in the possession of, or is 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.

Policy "What we have to do"
Principles developed by members of an organisation; should be linked back to legislation/regulation and set out how the local authority will implement legislation and regulation.

Procedures "How we do it"
Developed by an organisation to operationalise policy. This should reflect internal recording procedures and relationships between different sections of the department.

Subject Access
The right of a Data Subject to have access to their own personal data.

Contents

1. Introduction

Legislation
Under section 7 of the Data Protection Act 1998 (the "Act"), a Data Subject is entitled to access all personal data that a Data Controller holds about him or her, subject to certain exemptions. This is known as the right of Subject Access. Data Subjects are entitled to access their personal data within forty calendar days of submitting a valid Subject Access request.

Failure by the Data Controller to supply personal data within the time scales is a breach of the Act. Breaches of the Act may result in the Information Commissioner taking enforcement action against the Data Controller and may also permit the Data Subject to bring court action for compensation for distress caused.

As the Data Controller, West Sussex County Council processes personal data on service users and/or their families in both adults and children's services. West Sussex County Council has a statutory duty to provide timely access to an individual's data. This policy, along with accompanying procedures and guidance documents, has been developed to ensure that services are aware of their responsibilities in terms of effectively responding to Subject Access requests and providing access to personal data within the statutory timeframe.

During the writing of this document, reference was made to the Data Protection Act 1998; Legal Guidance on the Data Protection Act 1998, produced by the Office of the Information Commissioner; and BSI Data Protection guidance endorsed by the Office of the Information Commissioner.

Please contact the Data Management and Access Officer for further information about the Data Protection Act 1998.

The Data Management & Access Officer shall be referred to as "DMAO" throughout the remainder of this document.

2. Rights of the Data Subject

To access all their personal data
This is the case, unless specific exemptions apply.

To receive copies of personal data in permanent form
Data Subjects are entitled to receive details of their personal data in a permanent form. The Data Controller is not obliged to provide access to original documents or direct access to computer systems. However, rules may vary depending on the service that holds the data.

To receive personal data within 40 calendar days
The deadline for access is set from the point at which the Data Controller receives a valid Subject Access request. The DMAO must receive:

- A formal Subject Access request on the appropriate form [SSP 150];
- Two copy examples of evidence that confirms the identity of the requestor, one of which must be a photo ID;
- A £10 fee;
- Valid consent [Form of Authority] if the request is made via an agent [such as a solicitor or advocate].

It may also be necessary for the DMAO to consult with relevant members of staff from the appropriate service/department in order to be satisfied with the identity of the requestor. The DMAO will also need to be satisfied that any agent is indeed working on behalf of the Data Subject and acting in their best interests.

To have personal data explained if necessary
A Data Subject has the right to have personal data communicated to him or her in an intelligible manner. It is therefore the responsibility of the Local Authority to ensure that the Data Subject understands the data that they receive. If the Data Subject cannot clearly understand instances of data, action should be taken by the Local Authority to explain the data.

To be told the purpose(s) for processing
A Data Subject has the right to be told why his or her personal data is being processed. The second principle of the Data Protection Act 1998 requires that personal data should be obtained and processed only for one or more specified and lawful purposes. The right of Subject Access therefore enables the Data Subject to check that their personal data is being processed appropriately and only for the purposes for which they have given their consent.

To be told to whom the personal data is disclosed
The Data Subject has the right to know who has access to his or her personal data and who may ***may*** potentially have access to their personal data. Access to personal data must be consistent with the main purpose(s) for processing the data and comply with the permissions granted by the subject for the processing. Purposes for processing and rights of access vary depending on the service.

To have inaccurate data amended or removed
The Data Protection Act requires Data Controllers to process accurate and up to date personal data. Data Subjects have the right to request that inaccurate personal data is rectified, erased, blocked or destroyed. If a service department receives such a request, they should contact the DMAO for further discussion. The DMAO and service department may decide it is not appropriate or practicable for personal data to be amended or removed because it has taken steps to ensure the data is accurate. In this case, the Data Subject retains the right for the data to be supplemented with his or her own comments/objections to the data being held.

To authorise an 'agent' to apply on his or her behalf
An intellectually capable individual can authorise an agent (i.e. an individual, or an organisation) to access data on his or her behalf. The law in England does not explicitly state that an individual must be of a certain age to be able to authorise an agent. However, guidance from the Information Commissioner is that "by the age of 12 a child can be expected to have sufficient maturity to understand the nature of a Subject Access request". It is therefore WSCC policy that in most cases, children that are twelve years of age and understand the nature and purpose of Subject Access requests are old enough to authorise agents to work on their behalf.

3. Access to Personal Data

Receiving a Subject Access Request
Contact the DMAO as soon as you receive a subject access request. The DMAO is required to log the request on the corporate tracking system for legal and statistical purposes. If the request is in the form of hand-written letter or a verbal request, either the DMAO or the person who receives the request can send out a Subject Access Request application form [SSP 150]. Subject Access Request leaflets [which incorporate the application form] should be available in hard copy in most offices and should be on display in public areas where possible. Alternatively, there is a downloadable form on the Intranet under "Organisation>Access to Personal Social Care Information".

Supporting Identity Documentation
When the applicant returns their completed application to the DMAO, they must supply two forms of identity one of which must be a photo ID such as a passport or driving licence and the other a utility bill or similar. We do not accept original documents but do require good quality photocopies. The DMAO acknowledges receipt in writing and may consult the service department regarding the identity of the applicant if deemed necessary.

Access to Personal Data by an authorised agent
When an agent makes a request on behalf of a Data Subject, the relevant form [SSP 150] must still be signed by the Data Subject. The DMAO may still check with the Data Subject whether he or she is happy with the agent receiving the personal data and should highlight the implications of the request. If there is reasonable doubt about the validity of the consent, the request should not proceed until we are satisfied that it is a valid request.

Access to Personal Data of a Child
A parent or guardian may access personal data on behalf of their child if the child is too young to submit a request. If a parent has had parental responsibility ('PR') removed, this will impact on their right to access the personal data on behalf of their child. Also, staff should be aware that **in some cases it might not be appropriate to release the child's information to the parents**. Please contact the DMAO to discuss.

Access on Behalf of a Mentally Incapacitated Adult
Subject Access requests made on behalf of individuals that do not have adequate mental capacity can be made by those appointed to act on his/her behalf under Lasting Power of Attorney or by the Court of Protection. If the agent has no such power, the service must ensure that they act in the best interests of the Data Subject. Where an individual submits a Subject Access request on behalf of a vulnerable adult who lacks capacity, the DMAO must be careful to ensure the consent provided by the agent is valid and that the request is indeed 'on behalf' of the mentally incapacitated individual, and that the applicant has the best interests of the individual in mind. For ACD, those

who have been involved, or managed those involved, in casework for the client should provide informed opinions.

Access to Personal Data by Legal Agents

Any request received from an agent must be accompanied by signed Form of Authority [permission] from the Data Subject. No proof of identity for a Data Subject is required when the application comes from a professionally recognised agent such as a Solicitor. A payment is still required.

Access to the Personal Data of Deceased Individuals

The Act only covers the personal data of living individuals. (The data of deceased individuals is governed by the Freedom of Information Act 2000.) However, this does not mean that personal data of deceased individuals can be automatically passed into the public domain. Current WSCC policy is that it is assumed that the rights to access the personal data of the deceased individual generally fall to the next of kin of that individual, where appropriate. ACD should still have regard to any duties of confidentiality they owe to the deceased and should act in the best interests of that person's estate. Please discuss with the DMAO.

4. Roles and Responsibilities of Staff

The Subject Access process comprises a number of distinct steps that are further broken down into specific tasks. Roles and responsibilities are assigned accordingly and are outlined in this section. As Subject Access requests are time constrained, it is important that roles and responsibilities are understood.

A variety of staff roles are involved in the Subject Access process. However, the relevant service area retains overall responsibility for any subject access requests. Specifically, the key responsibilities and specialisms of the service areas are:

- To utilise knowledge of service users to make judgements about which data should be disclosed, based on Data Protection principles;
- To apply expertise in the areas of social work practice & relevant legislation
- To provide an appropriate point of contact during the Subject Access process:
- To ensure time scales are met.

Information Officer (Legal Services)
The Legal Services Unit is responsible for ensuring the County Council's compliance with Data Protection legislation. For this reason, the Information Officer in Legal Services is responsible for the following elements of the WSCC Subject Access process:

- Maintaining an overview of the corporate subject access tracking system
- Maintaining statistical information and producing IM reports
- Referring requests to the DMAO/ILO's in the relevant service area.
- Providing legal advice to the DMAO/ILO's and service areas.

The Information Officer also provides Data Protection training and advice to the Information Liaison Officers (ILOs) from each service area. The Information Officer and the ILOs also jointly provide relevant training to members of staff within their service area to ensure data is prepared effectively. The Information Officer cannot give legal advice to the data subject.

Data Management and Access Officer / Information Liaison Officer

- To receive and track all subject access requests for ACD.
- To advise of requests to the relevant service area, if appropriate
- To inform the relevant service area of the deadline for data disclosure;
- To advise the service area on specific data disclosure issues;
- To consult the Information Officer for legal advice when necessary;
- To alert the Information Officer [Legal Services] to problems that affect the carrying out of the process within ACD.
- To assist with relevant post-access enquiries regarding data accuracy;
- To update and improve the procedures and guidance within ACD over a specific time period, or as necessary;
- To support Office Resource Managers in their facilitation of the data preparation process.

Area Managers/Second Line Managers in ACD

- Occasionally making judgements as to how release of certain data items may prejudice the effective carrying out of statutory social work duties;
- Making final judgements about which data items should be withheld following consultation with the DMAO or Legal Services;

Social Work Team Managers and Social Work Practitioners

- To make judgements as to how the release of certain data items may prejudice the effective carrying out of statutory social work duties (i.e. likelihood of physical or mental harm occurring, as a result of the information being released) or to consider any breaches of confidentiality that may occur if data is disclosed;

Office Resource Managers

- To assist with the implementation and coordination of the process, where required;
- To coordinate the retrieval of data, as instructed by the DMAO;
- To photocopy data as required by the DMAO, or to allocate photocopying tasks to a member of shared support staff; or alternatively, to prepare data for scanning by ensuring files are appropriately and safely packed/boxed ready for collection by the internal courier service for the scanning process;
- To occasionally assist with the transfer of files around the county when appropriate as part of the Subject Access process.
- To seek general advice from the DMAO when necessary;
- To provide a shared support service to assist practitioners/DMAO with the administrative tasks of the subject access process.

5. Subject Access Process

Step 1 (Any member of staff)
If you receive a Subject Access request verbally or by telephone, take the name and address details of the applicant, and forward the details to the DMAO as soon as possible. You may ask the DMAO to send out an access application form/leaflet [SSP 150] or you may do this directly using the leaflet that is in local offices or download the electronic version that is placed on the intranet/internet. If you receive a letter requesting access, forward this to the DMAO as soon as possible.

Step 2 (Data Management and Access Officer)
Once the Subject Access Application form has been sent to the customer, the DMAO will record details of the customer and await receipt of the completed form.

Step 3 (Data Management and Access Officer)
Upon receipt of the completed form, the DMAO will check the supporting identity documentation, pay cheque into the appropriate departmental budget code; send an acknowledgement letter to the applicant; enter on the corporate tracking system; diary the 40-calendar day deadline date.

Step 4 (Data Management and Access Officer)
Use electronic information systems, [CIS / TCO/eRIC//Fwi] to identify location of data. Contact appropriate Area/Second Line Manager/Practitioner if necessary and appropriate e.g., the case is open.

Step 5 (Office Resource Manager/Data Management & Access Officer)
Liaise with the DMAO to arrange for the retrieval of all data relevant to the request (e.g. case files, system reports).

Arrange for the relevant data to be sent to the DMAO for electronic scanning by sending it via the internal courier system to:

Maggie Lucey/Judith Marsden
2nd Floor, East Wing
County Hall,
Chichester.

Step 6 (Data Management and Access Officer)
Where the information is to be scanned, the DMAO or a member of corporate shared support services will organise this with Swiss Post Ltd. When the scanning is complete, any files will be returned to the point of origin

Step 7 (Data Management and Access Officer)

Update the tracking spreadsheet upon completion.

Step 8 (Data Management and Access Officer)

It is a good practice recommendation that the DMAO or delegate contacts the data subject after they have had the opportunity to read their documents. This is to ensure that the data subject has no outstanding queries but particularly in instances where it is envisaged that some of the data disclosed may have revealed distressing events or circumstances to the data subject. It is out duty to recognise that accessing personal date can have have a profound impact on an individual and signposting to support services may be required.

Footnote 1: The Information Commissioner's Office has issued specific advice for 'social services' departments in respect of subject access requests. There is separate legislation relating to access to education records, health records and social services records. In practice this means that if the third party individual is an education, health or social services professional, information relating to them can be disclosed and they are not, therefore, regarded as 'third parties', as such. ***For further information see section heading Data Provided by Third Party Professionals on Page 20.***

6. Data Retrieval and Preparation

Retrieving Data
The following data stores should be considered during data retrieval, as more than one may contain the personal data of the client.

- Paper case files (open/closed)
- Electronic Recording of Information on Children system (ERIC or Fwi)
- Adult Information Systems (Fwi)
- Client Information System (CIS – historic post March 2011)
- Lotus Notes/CEMIS (E-mail system or any subsequent mail system)

Frameworki: A method of data retrieval on Fwi has yet to be determined.

TCO Systems: Currently, the most effective way of retrieving data from these systems is to run reports and to print hard copies which can then be scanned for editing in the same way as a regularised paper file.

The CIS: In the majority of cases, it is not necessary for data to be retrieved from the CIS. This is because the CIS is a management information system that stores data in duplication of that held on the case file. The CIS does hold important information about the location of files and indicates referral on to other systems.

E-mails: E-mails that contain the personal data of service users form part of the case record and therefore form part of the request. E-mails containing personal data of service users, and/or their family members, should be routinely printed and placed on the relevant case file (or copied and entered into any appropriate electronic system). Clients have a right to see copies of their own personal data, wherever it is recorded, and this includes data that is contained in e-mails.

Reasons for Data Preparation and Editing/Redaction
Social work case recording may involve the processing of personal data of more than one individual. This is particularly the case in older files. For instance, one diary sheet entry may contain the personal data of more than one client. Therefore data must be prepared to ensure only appropriate data is disclosed during Subject Access. The process of identifying and removing non-disclosable data is known as redaction. In relation to the Subject Access process, this means the removal of third party personal data recorded on the case file being requested. This is necessary if the data subject does not wish us to contact relevant third party individuals or the third parties have not provided their consent. ***[Please see following paragraphs for further details on Third Party Personal Data].***

Scanning and Electronic Document Editing

The Directorate has the facilities available to enable electronic editing of scanned material. Any requested data will be scanned and edited electronically.

7. Disclosable Data and Exemptions – General Guidance for data recording and handling under the DPA 1998.

Disclosable data is that which the client is legally entitled to see and which forms part of their personal data. Material, which a client has already been party to can be released. For example, the minutes of a meeting where the data subject was an attendee.

We do not have a responsibility to disclose material that the data subject already has a copy of or material that has already been disclosed to the data subject, perhaps by a previous subject access request. Occasionally, this is requested, and depending on the circumstances, we may re-supply information.

Third Party Personal Data
The data subject is not entitled to see the personal data of third parties [i.e., anyone else] without the third party's consent unless it is reasonable in all the circumstances to disclose it without their consent. Please discuss this with the DMAO if you want advice or more detailed guidance about this subject.

Not all detail constitutes third party "***personal data***" and a logical view can be taken of some data that may, for example, be already known by or shared with the subject or could reasonably be expected to be known by the subject i.e., the name of a sibling but not necessarily their current address or circumstances.

Sensitive Personal Data
When considering the personal data of third parties, and trying to gauge its relevance to the main client, it is useful to bear in mind the definitions of sensitive personal data, as defined in the Act. The Act identifies that sensitive personal data is that which consists of information as to:

- The racial or ethnic origin of the data subject;
- His or her political opinions;
- His or her religious beliefs or other beliefs of a similar nature;
- Whether he or she is a member of a trade union;
- His or her physical or mental health or condition;
- His or her sexual life;
- The commission or alleged commission by him or her of any offence, or, any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings or the sentence of any Court in such proceedings.

Seeking Consent from Third Party Individuals [Personal]
The data subject should be informed that we might need to contact other individuals about whom personal information is recorded on their file and seek their consent to share their data with the data subject. This may include family members and friends. We may rely upon the data subject to supply us with up-to-date contact details for these people. If current contact details cannot be supplied, contact the DMAO who may be able to trace the relevant people or to advise on the relevance to the data subject of doing so. The data subject has the right to request that we should not contact certain individuals. For instance, a child might not want us to contact their parents. If this is the case, the data subject should be informed that some of the data may be redacted prior to the release of the file.

Data Provided by Third Party Professionals
There is sometimes a lack of clarity regarding the requirement of consent in the case of third party professional data. There is separate legislation relating to access to education records, health records and 'social services' records. In practice this means that if the third party individual is an education, health or social services professional, the information is regarded as information provided by a "relevant professional" and not a 'third party', as such. There is specific guidance relating to "relevant professionals" opinions on the Information Commissioners website, please see below:

A professional opinion about the data subject is their personal information and must be released except where any exemptions apply.

Information about the person that has been received from a relevant professional may often represent that professional's opinion.

In most cases professionals are likely to expect their name and business contact details to be disclosed. However, you should carefully consider any objections a professional makes to the disclosure of these details. This is especially important if there is a real risk that disclosure of this information would be likely to cause them, or any other individual, harm.

If you consider recorded data is contentious or you suspect the disclosure of it will cause specific problems, you may wish to seek the views of the named relevant professionals about what information from their contribution to your records could be disclosed and which information they would not wish to be disclosed. You should also explain clearly that, if they decide to refuse consent for all or part of any data, that their refusal must be based on one of the relevant exemptions [see below] to The Act. You should also explain that whilst you will consider their views, the final decision about disclosure rests with you as the data controller.

Physical and Mental Health Data

If case recording includes information on the physical or mental health of the data subject, whilst generally disclosable, you must consider whether disclosure is likely to have a detrimental effect on the data subject.

For older cases, where establishments no longer exist and consent cannot be given. These documents should be released without consent, if in the DMAO's judgement it is reasonable to do so. Third party personal data should be removed.

Court Reports

Court reports can be disclosed to the applicant if they were party to the proceedings of the report. For instance, if a court ordered the removal of a child from his or her parents, and the child or parents later requested access to the actual court order document, it would be acceptable to release this document. If a third party requests copies of the court proceedings (i.e. a person that was not party to the proceedings), then the individual/individuals party to the proceedings should be consulted for consent.

Police Documents

If the case file contains documents supplied by the police, consent should always be sought before disclosure except in the case where the applicant is directly addressed on the police document. For documents supplied by Sussex Police, send a copy of the documents to:

Data Protection Disclosure Officer
Corporate Development Department
Police Headquarters
Malling House
Church Lane
Lewes, East Sussex, BN7 2DZ

Exemptions

Below are the three exemptions that may be applied under the Act

Exemption: Statutory Instrument 2000 No. 415
The Data Protection (Subject Access Modifications) (Social Work) Order 2000 – (S.I. No. 415) states that personal data does not have to be released if in doing so serious physical or mental harm to any individual is likely to result and serious consideration must be given to judge if this is the case or not. This exemption may also be used if disclosure of data is likely to prejudice the carrying out of social work functions. We are still under an obligation to inform the data subject that we hold this information whether we are releasing it or not.

Exemption: Section 29 Crime & Taxation
If to release personal data would impact on the effective prevention or detection of crime, then the data is exempt and does not have to be released as part of the Subject Access process.

Exemption: Section 7 [4] Duty of Confidentiality Owed
If an overriding duty of confidentiality is owed to any individual, the data should not be disclosed. For instance, personal data should not be disclosed if:

- It was provided by a third party in the expectation that it would not be disclosed to the person making the Subject Access request;
- It was obtained as a result of an examination or investigation to which the third party consented in the expectation that the information would not be so disclosed; or
- If the third party has expressly indicated the information should not be so disclosed.

Please discuss confidentiality issues with the DMAO or the Information Officer (Legal Services) if necessary.

8. Data Access and Support

Subject Access Meeting
Due to the sensitivity of personal data processed by ACD the data subject may opt to receive their data by a personal visit to an Area Office to view the data in the presence of a practitioner. This method enables the Data Subject to directly ask any initial questions about the data, and receive support from the practitioner if necessary. It may be the case that the Data Subject discovers upsetting information that he or she has not previously been aware of. It may therefore be necessary for a practitioner to offer support at this point in the process. This role is usually fulfilled by an independent social worker.

It is good practice to prepare the following:

- Preparation of a brief summary/chronology of events
- Planning how to conduct the 'interview'
- Warning the Data Subject that reading the data might be upsetting
- Suggesting to the Data Subject that he or she brings a relative or friend
- Telephoning the Data Subject prior to access (if posting the data), to warn about the sensitive nature of the data.

Even where a Subject Access meeting takes place, the data subject will still want to take away permanent copies of their data.

Posting Data by Recorded/Special Delivery
Data subjects may also choose to receive their information by post to be read at home privately or with another chosen support network. If the data subject prefers to receive their information by post, then we still have a duty of responsibility to offer support if needed but this can also be offered over the telephone if the data subject is agreeable to this approach. If a data subject lives at a great distance from the disclosing office, it may be appropriate to advise them to contact their local social care service for support or a support network local to them.

Data Subjects personal information should only be posted to them by Recorded or Special Delivery and not via the regular postal system.

Disputes with the Area Office
In some cases, Data Subjects will have accessed their records as part of a concurrent complaint or because they are dissatisfied with the service that they received/are receiving, or they feel they have a dispute with members of staff involved in their case.

If this is the case, then the DMAO will need to liaise with the relevant manager regarding any outstanding data issues or if the recorded data is the source of the complaint.

WSCC Complaints/Customer Care Procedure

Where the dispute is only associated with the Subject Access request, then this should be resolved locally, escalating the relevant line management where necessary.

If the dispute concerns misplaced or lost files, inaccurately recorded data or challenges the use of exemptions, the DMAO will be need to be involved.

Closing the Request

Once the disclosure material has been received by the data subject and it is evident there are no outstanding issue, the corporate tracking spreadsheet will be updated and the Subject Access request will be considered closed.

9. Contacts

If the data subject is dissatisfied with the content of his or her personal data, he or she should contact the DMAO who will investigate the specific concerns. If the data subject has cause for complaint associated with the Subject Access process, he or she should pursue the matter through the appropriate Customer Relations Teams for the relevant service. If the data subject is not satisfied with our response, they may then complain to the Information Commissioner.

Data Management and Access Officer (DMAO)
Adults & Children's Directorate
Room 312
County Hall
Tower Street
CHICHESTER
PO19 1QT
Phone: 01243 777519/07595 964212

Children and Young People's Services Complaints Team
Children and Young People's Services
West Sussex County Council
County Hall
Tower Street
CHICHESTER
PO19 1QT
Phone: 01243 753880/Freephone 0800 137126
Email: CYPS.comments@westsussex.gov.uk

Adults' Services Customer Relations Team
Customer Relations Team (Adults)
Freepost
West Sussex County Council
County Hall
CHICHESTER
PO19 1RQ
Telephone: 01243 752164 Textphone 18001 01243 752164
Fax: 01243 752001
E-mail: as.complaints@westssussex.gov.uk

Office of the Information Commissioner
Wycliffe House
Water Lane
WILMSLOW
SK9 5AF
Telephone: 0303 123 1113
Fax: 01625 524510
E-mail: casework@ico.gsi.gov.uk