HOW ACTION FOR CHILDREN WORKS

Policy Name: Access to Personal Information and Individual's Rights Policy and Procedure
Policy Group: Core Children's Services
Last updated: 20 August 2018
Date to be reviewed: 01 April 2018
Current Contact: Pera Svilar - Information Governance Officer

Access to Personal Information and Individual's rights

Policy and Procedure

Policy Name: Access to Personal Information
Policy Group: Core Children's Services
Last updated: 19 April 2017
Date to be reviewed: 01 April 2018
Current Contact: Pera Svilar - Information Governance Officer

Contents

Policy Name: Access to Personal Information
Policy Group: Core Children's Services
Last updated: 19 April 2017
Date to be reviewed: 01 April 2018
Current Contact: Pera Svilar - Information Governance Officer

Policy Name: Access to Personal Information
Policy Group: Core Children's Services
Last updated: 19 April 2017
Date to be reviewed: 01 April 2018
Current Contact: Pera Svilar - Information Governance Officer

Introduction

Chapter III of the GDPR gives Individuals Rights these rights are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The Charity has a duty to respond to all requests it receives. This policy describes the actions to take to process and respond effectively and efficiently to any request received. Requests should be logged with the Information Governance Officer, verified, acknowledged and responded to within a calendar month.

1. The right to be informed

Action for Children uses a Privacy Notice's sometimes known as Fair processing notices to inform individuals about how their information is processed see the Data Protection Policy and Procedure where this right is covered in detail.

2. The right of access

Action for Children holds a significant amount of information relating to individuals, in the form of structured files such as case and employee files, and also in emails, electronic files, and databases. Under the right of access, we have to make almost all of this information available, upon request, to the individuals to whom it relates.

This document provides a framework for decision making and signposts employees to external guidance in order to ensure compliance with the Data Protection legislation and best practice, and to maintain consistency with statutory and other voluntary agencies when sharing information. Action for Children are the only major children's charity to have signed the Information Commissioner's Office's (ICO) Personal Information Promise, underlining our commitment to protect personal data – see the Data Protection Policy for more information. The six Caldicott Principles should also be applied by health and social care parties when considering whether personal information should be shared.

Children's Services should also refer to Information sharing: advice for practitioners providing safeguarding services (March 2015) from the Department of Education (DOE) which is

applicable to all four nations in the UK. In addition, project staff must ensure that **wherever personal information is collected from the service user, they are aware of this position and a copy of the Keeping Your Information Safe and Secure leaflet (Appendix 1) is made available to them. The consent of the service user must be sought, to collect and process their information, a completed consent to process form (Data Protection Policy Appendix six) must be available as evidence.**

Accessing personal data for audit or research purposes by third parties without the prior consent of the individual is unlawful. If consent cannot be obtained to process data for these purposes then the information should not be included or alternatively redacted so that any personal data capable of identifying the individual(s) service user is removed. Where third party organisation's are used as auditors, researchers or subprocessors of personal data a contract and a Data Processing Agreement (Data Security Policy: Appendix five) must be in place, it is recommended that an Information Sharing Agreement (Data Security Policy: Appendix ten) should also be produced and provided for use by the third party.

Section 1 of this policy applies to any request made by or on behalf of a service user or related individuals. Section 2 applies to requests made by other individuals about whom the organization may hold data. Section 3 applies to requests from the police, other agencies and third parties.

2. Requests by service users

Requests by or on behalf of service users are known as Subject Access Requests.

2.1 Receiving a request

Requests have to be made in writing, but this can include email or text messages and potentially include social media sites like Facebook and Twitter.
Technically, requests can be made to any employee, but they are most likely to be made to someone working directly with a service user, or to the service itself via a Business Support Officer (BSO) or manager.

Requests do not have to quote the Data Protection Act to be valid. Some requests may erroneously quote the Freedom of Information Act 2000 (which only relates to information held by public authorities and relates to non personal data). The organization will still be required to process such a request under the Data Protection Act where it has erroneously been named a Freedom of Information Request.
Occasionally Action for Children are asked to assist a Local Authority with a Freedom of Information Request the request should be sent to the Information Governance Officer and the Operations Director for the service to assist and respond to the request.

Requests should be passed on to the Children's Services Manager (CSM), who may then deal with it themselves, delegate to a worker or, if the case is not related to their service, pass it to the Access to Records team. Details of the request must also be shared with the Information Governance Officer for central recording and reporting.

Sometimes, a request may come in to the Action for Children website or through one of our national offices. If the request relates to an open case or service, the request will be forwarded on to the CSM. If the request relates to a closed service or a historical case it will be handled by the Access to Records Team. If the request is related to a Safeguarding investigation it should be referred to the Action for Children's safeguarding lead.

2.2 Requests on behalf of others

Individuals can nominate others to make a request on their behalf. This is often the case where an individual is making a complaint about a service they've received, or if they are involved in a dispute or care proceedings with Local Authorities. Often, the request will be made by a solicitor.

We have to ensure that such requests are valid and are actually being made on behalf of the individual, written and signed consent should be requested, and, if necessary, the individual should be contacted directly by the service to make sure.

Basic Rules of Subject Access

1. The individual making the request must be the individual or their representative (including a parent or solicitor), and must be able to prove this (providing ID or signed consent);

2. There is an assumption that the individual has the right to see the data we hold;

3. We have to respond to the request within 40 days or one month under the new legislation (from 25th May 2018). There is an option to apply for an extension of up to two months as long as this is done within one month of receiving the request. Extensions will only be granted where the request is complex or there has been numerous requests from the same individual;

4. We are required to provide data 'in a concise, transparent, intelligible and easily accessible form.' That means we should use clear plain language;

5. We should not place an individual at risk of harm in providing data - either the individual making the request, or anyone else.

2.2.1 Parental requests

Parents may also make requests on behalf of their children. In these cases, the age and competence of the child should be taken into account. It is recommended that a child the age of 13 or above is sufficiently competent to make a request in their own right, and in particular if the service is of a confidential nature, their consent should be sought before a request from their parent is accepted as legitimate.

2.2.2 Family break-ups

Unfortunately, in some cases where families have broken up, one parent may use a request on behalf of their child to try and gain information relating to the other parent. In these cases, although the request is legitimate, extra care should be taken to ensure that any information relating to the other parent that is not directly related to their child should also be removed.

2.2.3 Parental responsibility

In all cases where a parent is making a request for their child's data, we must confirm that they have parental responsibility for their child. Mostly this will already be known. However,

where a request is made in relation to care proceedings, or the service is aware of anything which may mean that parental responsibility is unknown or has been removed, this should be checked with the parent, and if necessary the Local Authority prior to information being provided. Where possible we should request to see a copy of the birth certificate and any parental responsibility agreement. A parent who has had Parental Responsibility removed for any reason does not have the legal right to make a request on behalf of their child.

2.2.4 Local Authorities and Parental Responsibility
Where a child is placed in the care of a Local Authority or other agency, the right to make a Subject Access requests follows that placement. Therefore, a request by that agency for access to data in relation to a child in their care should be handled as a Subject Access Request from a parent, rather than an information sharing request.

2.2.5 Safeguarding
Where a service is aware of a safeguarding issue indicating that a child may be placed at risk by providing their information to a parent, the information should be withheld.

2.2.6 Court Orders
Where we are ordered to provide information to a parent or their representative by a court, we are required to do so. If there are safeguarding issues involved, this should be made clear to the court in providing the data and representation to the court may be made that the information should be viewed by the judge *in camera* (in private), however it is the court's decision how the information will be handled once a request has been fulfilled.

Case Study #1
A mother is attending a parenting group at a Children's Centre. Her child's father places a Subject Access Request on behalf of himself and the child. The father is estranged from the mother and is not resident, however he does have parental responsibility for the child.

The father can be provided with information relating to the child, but all information relating to the mother must be removed - this may mean copying it into a separate document.

Additionally, if any information relates to the father, this may also need to be provided to him, although this will depend on whether

2.3 Fulfilling a request

Requests have to be answered with <u>one month</u> of having been received. This can entail quite a lot of work, however if we don't meet the request the individual has the right to make a complaint to the Information Commissioner's Office, which can lead to enforcement action against the organization and financial penalties being imposed

2.3.1 What we have to provide

a. Any personal data which **directly relates** to the individual
b. Any personal data which has been provided by a third party who was **acting in a professional capacity**
c. Any personal data which was provided by another third party:

i. where there was **no expectation of confidentiality**, *or*
ii. **consent has been gained** from the party that provided the data*, or*
iii. where not providing the information would be of **significant detriment to the individual requesting access**, and of less detriment to the individual who provided it.

2.3.2 Information which relates to the individual
The majority of information we hold, particularly in a formal case file, will relate directly to the individual making the request. It will be things like registration forms, running records, observations and reports. These will usually be provided in full.

Information may also be held in other ways - emails, for example. These should also be provided - they can be printed off or copied in to a separate document, providing sender and recipient data is also copied.

Unless there is a known risk to workers from the individual making the request, names of employees should not be removed - as professionals, it is expected that information they have recorded should be of a standard which can be provided to the person to whom it relates.

We are also required to disclose where we have shared information with other agencies. However, where this may prejudice an ongoing investigation (such as a Safeguarding investigation by the Police or other agency) information relating to that should be withheld.

2.3.3 Requests for information which includes data about other individuals
Responding to a SAR may involve providing information that relates both to the individual making the request and to another individual. The Act states that organizations do not have to comply with the request if to do so would mean disclosing information about another individual who can be identified from that information, except where:

- the other individual has consented to the disclosure
- it is reasonable to comply with the request without that individual's consent.

The decision to disclose data relating to a third party will involve balancing the data subject's right of access against the other individual's rights in respect of their personal data. If the third party consents it would be unreasonable not to share data but if not, the Charity must decide whether to disclose the information anyway.

The Charity cannot refuse to provide subject access to personal data about an individual simply because it was obtained from a third party. The rules about third party data apply only to personal data (not who supplied the information) which includes both data about the individual who is the subject of the request and a separate/third party outside of the request.

2.3.4 Information from people who are not professionals
The last of these criteria may be especially complicated. The simplest approach to this type of data may be to ask for the consent of the third party to provide access to the data - however, if you do this it must also be clear that we may have to make the decision to provide the data irrespective of their consent or refusal.

For example, a neighbour or family member may have provided information to us about a child or parent, but on the understanding that it would not be shared. That information was significant but could not be verified, and may cause significant detriment, for example may play a role in care proceedings.

In that case, providing there is no risk to the child, it may be appropriate to provide access to the information to enable the parent to refute the information. However, if there was a risk that the parent might cause harm to the person who provided the information, the information would not be provided.

This type of decision is known as a balance of interests, and if there is a doubt as to how it should be applied, please seek advice from the Information Governance Officer.

2.3.5 Information from professionals

Individuals who provided data in a professional capacity do not have the same level of protection - there would need to be a clear risk of harm to them or another individual in order to withhold the information.

However, it is appropriate to inform them or the agency they work for that we received the request and that we intend to provide a copy of the information, giving them a timeframe within which to lodge any objections. In doing this, it should also be made clear that the final decision as to whether to provide the information rests with Action for Children - any objection may be taken into account but only insofar as the law allows.

2.3.6 Risk of harm

The law allows us to withhold information where there is a risk of harm to any individual. This may be physical or emotional harm. In particular this applies to social care and health records. Information from professionals should be taken into account, especially in providing medical information. Any risk of harm should be thoroughly documented, as the requestor must be told of the decision to withhold any data, and may well challenge the decision. This exemption is only partial - as much information as can be provided safely should be. The exemption is provided under Statutory Instruments which may be quoted if required[1].

Please note that risk of harm to the organization or an employee, in terms of reputation or legal action, is not grounds to withhold information. If you believe there to be a reputational risk attached to a Subject Access request, please escalate the request to your Operational Director and the Information Governance Officer.

We also cannot restrict access to information based on any other use that the individual may wish to make of it - for example publishing it online - unless there is clear evidence that doing so would lead to harm.

2.3.7 Commissioned services

[1] The Data Protection (Subject Access Modification) (Social Work) Order 2000 and the Data Protection (Subject Access Modification) (Health) Order 2000.

In some commissioned services, we are required to pass any request for information on to the commissioning body - typically where we are recording information on their systems, or they are very tightly in control of the service being delivered. This arrangement will usually be indicated in your service contract.

Where this is the case, we should acknowledge receipt of the request and state that we are legally required to pass the request on to the service commissioner, who will respond according to their own procedures.

Whilst Local Authorities request that Action for Children projects and services sign local Information Sharing Protocols (ISPs), these cannot be used to force the Charity to share information where this would otherwise breach the DOE or ICO guidance or the Act. Where a decision to share information cannot be made at a local level, advice must be sought from the relevant line manager, with support from the Information Governance Officer or the Head of Safeguarding.

2.4 Preparing the information for access and redaction

Information should be presented in as full and transparent a way as possible, with any acronyms or codes translated. Duplicate information can be removed. If other information must be removed, the reason for the removal should be clearly marked. Where a document will be redacted to the extent that it will not be intelligible, the whole document may be withheld, though this must be stated in the cover letter. Redaction means deleting information, to which the data subject (the individual who has made a SAR) is not entitled, from the personal data that are to be released to him/her in response to his/her SAR.

There are a number of ways to remove information where this is necessary:

- Photocopying - make a copy of the original data, and black out the section to be removed with a permanent marker, then make another copy. **The text MUST be fully obscured on the second copy;**
- Use of redactable tape to cover section to be removed as above;
- Re-typing - we have to provide a copy of the information, not a particular document; it may be helpful to copy-type the data into a fresh document, especially where there is a lot of data to be removed;
- Digital editing - where the document to be redacted is an electronic image such as an adobe PDF or JPEG, the document can be blacked out using software such as Adobe Acrobat, Photoshop or even Paintbrush. The document should then be saved as a new document, printed out and then rescanned so as to remove any metadata capable of being used to undo the redaction.

When redacting electronic records:

- Open the document in Microsoft® Word and use a solid black drawing shape to cover the text to be redacted (alternatively remove the text entirely).
- Convert the Word document to PDF. The drawing shape gets converted and cannot be deleted from the PDF so it seems secure. However, it is vulnerable at this point to an interested party selecting all the text around the redacted area and pasting it into an application like Word or Notepad. The text under the black box is revealed in its entirety.

More sophisticated users can use a metadata-revealing application to access all prior revisions to the document, which also are embedded in the PDF.

- Printout the resultant file saved as PDF and then the hardcopy back in as a PDF. The print and scan removes the metadata and underlying text, producing an image of the redacted document.
- Release the re-scanned document.

If information is only held in an electronic document, the original document must not be overwritten in the editing process. However, it is permissible to remove sections of a Word document for example, provided that this is stated in the new version.

It is good practice to provide information in the same format that the individual made the request, although it is not strictly required; so if a request was emailed in, information should be made available electronically; likewise if a request was mailed in, the response should be on paper. However, if doing this will incur a great deal of work or cost, this is not required. New legislation requires us to provide the information in a commonly used electronic format that is if the request was made electronically then we should also respond electronically. However if the request has been made through a social media site then it would be inappropriate to respond using that format and in those circumstances an email would be preferable.
If the document has been generated by Action for Children, if its originator is available then they are responsible for redacting the information because he/she will be best placed to decide what can and cannot be released in accordance with the Act. If the information does not originate from the Charity or the originator is not available, then the data owner, or in cases where it is no longer possible to contact the data owner, the holder of the information must be asked to decide whether any redaction is required. Data holders must keep a copy or a comprehensive record of what was provided to the data subject, together with the reasons for redaction, in case their decisions are subsequently challenged.

If the SAR has not requested names then they should be redacted as they are not relevant to the information requested. The accompanying letter should state "the names and contact details of individuals have been removed as they are not a substantive part of the information you requested." If the names are a central part of the information requested, then an exemption may have to be used to withhold the names. You should contact the Information Governance Officer to discuss which might be the most applicable exemptions to use. Exemptions may include:
• S38 - Health and Safety
• S40 - Personal Information
• S41 – Information provided in confidence
• Section 28 – National security - see paragraph 7 below
• Section 29 – Crime and taxation
• Subsection 33 – Research, history and statistics
• Schedule 7 – Miscellaneous exemptions, paragraphs (1) – Confidential references given by the Data Controller, and (10) - Legal professional privilege and other paragraphs.

Requests that may fall into this category may include requests for staff lists or directories, names of staff who attended a specific meeting or a copy of an organizational chart. The

names of some senior officials and their responsibility for a particular subject are already made public. In these cases it may be inappropriate to withhold the details. As a general rule the names of officials below the Executive Leadership Team, should be withheld unless an individual is in an outward public facing post and their name is already in the public domain.

2.5 Providing access

With the exception of Adoption cases, access may be provided by simply sending the information to the individual. If this is the preferred option, it must be done securely, for example by encrypted email or tracked postal service but remember that recorded delivery is not a tracked postal service.

If you are still working with the service user, or in the case of particularly detailed or challenging information, it may be helpful to ask the individual to attend a meeting to view the information. This allows the opportunity for the individual to ask any questions that may arise, and to discuss the content of the information.

Offering a meeting and counselling is a legal requirement for Adoptees requesting access to their data, and information can be withheld if the offer is not taken up. However, attending a meeting is not a requirement for any other service user, and where a meeting is offered and refused we are still required to provide a copy of the data.

Where a meeting is held, it should be conducted in a way that puts the service user at ease. They may wish to be accompanied, and the employee leading the meeting should have sufficient understanding both of the information and the context of the service to answer any questions that may arise.

Sometimes reviewing personal records can lead to safeguarding disclosures. Where this occurs, the Safeguarding policy should be observed as would be the case for any other disclosure of this nature. If the disclosure is of a historical nature and relates to services provided by Action for Children, the Historical Abuse Policy should be followed and the Safeguarding Manager informed.

2.6 The Access to Records Service

Action for Children's Access to Records Service was established to handle requests from former service users and their families. They have particular expertise in adoption, fostering and residential care cases, and also undertake some work on Genealogy requests (see below).

Requests relating to any records from closed services can be referred to the ATR service at the request below. They are also available for advice and support, along with the Information Governance Officer.

Due to limited resources, managers and employees with appropriate experience may be asked to undertake work on behalf of the Access to Records service. Additional information may be provided at that time, although this policy will apply in the majority of cases.

2.6.1 Requests by relatives for service user information

With the exception of parents acting on behalf of their child, we have no legal obligation to disclose information relating to a living service user to a relative. In fact, where the service user is still alive, we would be breaking the law in doing so. Therefore, for open cases, no access should be provided to relatives unless directed by the Courts.

However, particularly for long-term records and where a service user is deceased, we often receive requests from relatives. These are often referred to as Genealogy requests, and are made by the children or other close family of people who may have spent significant periods of time with Action for Children when we were known as National Children's Home. The information we hold about their relatives will contain important family history and as such we can provide access to this data where resources allow, though there is no statutory obligation to do so.

Where a service receives a request, it should be referred to our Access to Records team.

3. Requests by employees, volunteers, carers and donors

Under the Data Protection legislation, any Data Subject can submit a request for access to their personal data. It is increasingly common, especially where there is a dispute of some kind, for employees, and others working with the organisation such as carers, to make such a request.

The same basic rules apply to any Subject Access Request, regardless of who has made the request. However in addition to these there are specific extra rules covering negotiations, business planning or where information is supplied by peers and in strict confidence.

Particularly in the case of requests from employees, carers and volunteers, the right of Subject Access will be exercised as part of other ongoing processes and may be problematic for the organisation and emotive for the individual. Requests should be handled with care. Request from employees will be managed by HR and must also be reported and logged with the Information Governance Officer.

3.1 Receiving a request and preparing material

As with service user requests, a request can be made to any employee within the organisation, and via any written media.

However, due to the nature of many requests they are likely to be made to a more senior level of the organisation, often with legal support, for example from a Trades Union or solicitor.

In all cases, care should be taken to limit any conflict of interest which may occur; for example, if a line manager is providing a great deal of personal data relating to the request, they should not be directly involved in deciding what data is included and redacted from the response.

Basic Rules of Subject Access

1. The individual making the request must be the individual or their representative (including a parent or solicitor), and must be able to prove this (providing ID or signed consent);
2. There is an assumption that the individual has the right to see the data we hold;
3. We have to respond to the request within one month under the new legislation. There is an option to apply for an extension of up to two months as long as this is done within one month of receiving the request. Extensions will only be granted where the request is complex or there has been numerous requests from the same individual;
4. We are required to provide data 'in a concise, transparent, intelligible and easily accessible form.' That means we should use clear plain language;

For employee requests, HR advice should be sought and HR will directly handle the collection and preparation of the information to be disclosed. For carer or volunteer requests, a senior social worker may be used.

In all cases where there is a risk of complaint, litigation, or where the request is part of a wider issue such as a disciplinary or grievance process, the Information Governance Manager should be informed and/or consulted.

Where you need to redact (remove) information from documents, the reason for this should be stated in a cover letter as part of the response. Information should then be provided, if possible, in the same format that the request was received.

Information should be sent by as secure a means as required according to the content.

3.2 What can be requested?

Any data which relates to an individual can be requested by them. Although some information will be held solely on paper and in unstructured files, this type of data is very rare. Typically, information is created on computer or ends up being stored that way, and can therefore be requested by the individual to whom it relates.

We will need to provide details of whom the information has been shared with - for example if the information has been passed to Ofsted, a Local Authority or the police. However, this should only be disclosed where doing so would not prejudice an ongoing investigation.

3.2.1 Emails

Particularly in disputes, emails are often sought as a way to see people's opinions and actions in respect of an individual. Email conversations which discuss an individual, even using code (for example initials or a number), are subject to disclosure to that individual. This will also apply to Lync and other instant messenger-type software where data is stored beyond its immediate use.

Where a request seeks the disclosure of emails, the simplest way to gather them is to ask people to forward any emails relating to that person to one central co-ordinator. However, in cases where there is a risk that the organisation may be accused of destroying data to avoid embarrassing disclosures, it may be more appropriate to ask IS provide copies of mailboxes to whoever is coordinating the response, so that a chain of evidence is maintained.

3.2.2 Personal Files

In most cases of this type there will be some form of file relating to the individual, whether this is held as a physical file or electronically. In most cases, the whole of this file should at least be considered for disclosure as it is the official record of the individual's involvement with the organisation.

It is acceptable to carry out routine file maintenance (removal of expired disciplinary sanctions for example) prior to providing access if this would have occurred anyway, however no other information should be removed.

3.2.3 Request for CCTV images, digital images and photographs

The Closed Circuit Television Code of Practice (Appendix Two) provides further information but individuals asking to see any of the above must be asked to provide a photograph as part of the initial authentication procedure. Times and locations when the data subject's image were purportedly caught on CCTV will also be necessary.

Images captured digitally or on CCTV will need to be carefully reviewed. If the data subject is part of a group of persons then the identifiable images of other persons should be redacted unless consent can be sought, if feasible. Any redaction must be carried out electronically by the holder of the equipment. Where practicable, the individual should be asked if they would be satisfied with merely viewing the images recorded but travel and other expenses must be met by the individual.

3.2.4 Information from managers or corporate advisers

In particular where there is an ongoing dispute relating to the individual, information from line managers (or equivalent) and advice from departments such as HR is likely to form a significant part of the data which the individual is trying to gain access to.

Due to the nature of the relationship between the individual and these parties, there can be no expectation of privacy; they are deemed to be in a position of authority over the individual and therefore any opinion or advice they have expressed will be subject to disclosure, even where it may be embarrassing for individuals - or the organisation - for this to happen.

Even where there would normally be an expectation of confidence - for example in Supervision between two line managers - discussion and decisions recorded in relation to an individual may be viewed by that individual. The only exceptions to this would be where an individual would be placed at risk of harm due to disclosure, or where advice provided has been purely procedural in nature, rather than relating specifically to the individual.

An exemption may apply in the case where discussions between managers and/or advisers forms the basis of a negotiation or management planning with or related to the individual which would be adversely affected by disclosure - however, due to the limited scope of this exemption, advice must be sought from the Information Governance Manager before it is relied on to prevent disclosure.

3.2.5 Information from colleagues

Information provided by, or which also relates to colleagues and peers is in a different position to that provided by managers. It is considered as true third party information, and each party is equally protected under the DPA. As with service user requests, it may come down to a balance of interests between the parties, although factors like duties of confidence will also need to be taken into account, as will the risk to individuals involved.

In some circumstances there will not be an outcome which does not cause problems for one party; there is a likelihood that the party that does not get a decision in its favour will complain, either internally or to the ICO. Decisions of this type should therefore be made in consultation with the Information Governance Officer.

Case Study
An employee is accused of a disciplinary offence and colleagues have provided statements relating to the incident in question. The employee is concerned that the statements may be untrue, so they make a Subject Access Request asking to see the statements.

The statements were made in confidence, and the individuals withhold consent. However, due to the fact that the individual could be dismissed based on the allegations in the statements they would suffer significant detriment if they were not given access to the data. Additionally, elements of the data would be required to be provided under the rules governing disciplinary and tribunal processes.

Therefore the data should be provided, although it may be necessary to redact (remove) some parts which directly identify the other party.

In some circumstances there will not be an outcome which does not cause problems for one party; there is a likelihood that the party that does not get a decision in its favour will complain, either internally or to the ICO. Decisions of this type should therefore be made in consultation with the Information Governance Officer.

3.2.6 References
There are specific rules governing references, however generally a reference will be seen by the individual to whom it relates if they ask the right party. Therefore, there is little point in withholding them if they are requested.

If we have provided a reference, we do not have to provide the individual with a copy of it. However, the recipient of the reference does have to provide a copy. Likewise, where we have received a reference, we are obliged to provide a copy.

Where references are provided or received 'in confidence' it should be clear to the provider that that confidence only extends as far as the individual the reference relates to has not suffered significant damage or distress as a result of their reference - for example in losing a job. In those circumstances, if the individual requests access to their reference, the balance of interests means it would be disclosed.

This applies equally to employment and other types of reference. Additionally, in all cases where a reference is an expression of professional opinion, the reference would need to be disclosed.

3.2.7 The One Month Rule
Under the DPA, we have to respond to a Subject Access Request 'as soon as possible and in any case within one month. Failure to do this may result in enforcement action by the ICO and the individual being awarded compensation.

However, where a request relates to other ongoing processes, it is acceptable to use the whole one month period to respond to the request. We can also ask an individual to clarify the location of the information they are seeking - for example providing a date range to search within, whether they want their file, emails, etc., or (for volunteers or carers) the name of the service they were working with. The one month does not begin until we have received a response to such a request.

We can seek an extension of up to two months as long as this is done within one month of receiving the request. Extensions will only be granted where the request is complex or there has been numerous requests from the same individual;

3.2.8 Health Information
Health information may be held for a number of reasons, particularly in relation to carer and employee files. Under a Statutory Instrument, where we are holding detailed medical information we are required to check with a medical professional before disclosing it, in order to prevent harm to the individual.

Specifically this may relate to reports from General Practitioners or Occupational Health Reports. Ideally, the medical professional who provided the data should be consulted. Where this is not possible, another qualified professional may be consulted.

In any case where the professional opinion states that the information should be withheld, this should be noted in the cover letter accompanying the response. Consultation with the relevant professional must be completed within the one month period.

3.2.9 Requests and litigation – privilege and civil procedure
In some cases, requests may be a precursor to a legal action and this should be born in mind when considering what may be disclosed. This can work in several ways however.

Generally, the courts have not enforced SARs which are sent in as a precursor to legal action, however the ICO's view is that they are valid and enforcement action could be taken against an organization refusing to disclose, and there would also be nothing to stop an individual asking a County Court to enforce disclosure, which would incur costs to Action for Children to defend.

If an individual or their representative informs us that they are considering action in which Action for Children is a party, their request may also have legal force under the Civil Procedure Rules on disclosure, under which we have a duty to disclose all relevant material . This may actually lead to more information being disclosed than would be under a SAR, although not immediately; the parties have a duty to retain documents likely to be required for the purposes of litigation, which may then be disclosed upon request at a later date.

If we are aware of litigation or that it is a likelihood (for these purposes it must be a probability not a possibility), any communication between a lawyer and client, and any document specifically created for the purposes of litigation is also covered by litigation privilege. For these purposes, paralegals and other legal advisors are not covered by the communications aspect of this privilege unless supervised by a lawyer.

In addition, any communication in respect of an employee which is conducted with a lawyer will be covered by legal privilege and so is also not disclosable under the Subject Access provisions. This may be particularly important in respect of Employee Relations cases. Again, this does not extend to paralegals and other legal experts who are not supervised by a lawyer.

3.2.10 Exemptions

The Act details a number of exemptions to the obligation to disclose personal data and those considered most relevant to Action for Children are summarised below.

Confidential references	References given by the controller that are connected to actual or potential education, training or appointment of the data subject. This does not apply to references from a third party source.
Legal Privilege	Documents that are subject to legal professional privilege.
Management forecasts	Data used for an organisation's forecast or planning to the extent that disclosure would prejudice the organisation's ability to conduct its business.
Negotiations with the individual	Information which relates to ongoing negotiations between the organisation and the individual requesting the information, where disclosure would prejudice those negotiations.
Prevention or detection of crime	Any information if its release would prejudice: • the prevention or detection of crime • the apprehension or prosecution of offenders • the assessment or collection of tax, duty or similar imposition.
Repeat requests	Identical or similar requests do not need responding to unless a reasonable time has elapsed or there is a reasonable circumstance.
Third Party Information	An organisation cannot refuse to provide access to personal data because the data refers to a third party source. Instead, the organisation must undertake a 'balancing act' to ensure the privacy rights of the individual requesting data and the third party included the data are respected. It may be possible to: • anonymise the data relating to the third party • seek consent from the third party • decide if disclosure is reasonable, considering any duty of confidentiality owed to the third party or statutory requirements.

In addition, we do not need to provide data which was deleted (distinct from archived, which is included) before the request was made, or created after it was made. This limits the scope of requests so that it does not include information which may develop during other processes - although technically, the individual could then put in a subsequent request for this information.

3.3 Requests from ex-employees, carers or volunteer

When and individual's relationship with Action for Children comes to an end for any reason, their personal data will be archived for a period of time. During that time the individual can still request access to their data according to the rules above.

Ex-employees will typically approach the organisation centrally for their data. This request should by forwarded initially to HR Shared Services. They will then be able to establish the location of the individual's records.

Volunteers and carers are more likely to contact the service which they worked with, and the request should be handled by that service, where it is still in existence. Where it is not, volunteer requests should be passed to the Volunteer Manager. Carer requests should be escalated to the local Family Placements Manager.

3.4 Donor information

Donor and supporter information will typically be held solely by Fundraising. Any requests relating to supporter information should be passed to the Supporter Care team. The same rules apply as to all other requests.

4. Requests from the police, agencies and third parties

4.1 Requests for information from the police

Under the Act (Sections 28(1), 29(3) and Schedules 2, 3), the police have a right of access to personal data held by Action for Children. Each police force in the UK has a specific section 28(1) or section 29(3) form which relates specifically to requests of personal data from external organisations. The form should be completed by the officer making the request and signed by a senior officer before it is sent to any Action for Children project. This form should be addressed to a specific individual within the Charity.

The form issued by police will certify that the information is required for an investigation concerning: national security, the prevention or detection of crime or the apprehension or prosecution of offenders, and that the investigation would be prejudiced by a failure to disclose the information. This provides Action for Children with a legal basis for supplying the data under the Data Protection Act exemptions.

4.2 Requests via other agencies

In some instances, we may receive requests from other agencies where we have provided them with information about an individual who is now requesting access to their data. These requests will typically include a copy of the information we have provided and provided a short time frame in which we will need to state whether or not the information may be disclosed.

In all cases, the information we have provided will be in a professional capacity, and we should provide consent for it to be release. Only where we believe an individual would be put at risk by the information being disclosed should we make any objection. We can remind the

agency that any disclosure is subject to their compliance with the Data Protection Act, especially in terms of removal of third-party data. Any request like this should be handled without delay.

Requests by other agencies for access to personal information should be dealt with according to the Information Sharing and Confidentiality policy and the HM Government publication *Information Sharing: Guidance for Practitioners and Managers.*

4.3 Requests for information from third parties

The Data Protection Act does not prevent an individual making a SAR via a third party such as a solicitor acting on behalf of a client. Under these circumstances, employees need to be satisfied that the third party making the request is entitled to act on behalf of the individual but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. Where a Solicitor supplies a signed copy of a written authority, unless the employees can certain that the signature is that of the correct service user, they will need to either:

- Confirm the request with the service user where possible or with the individual who has statutory responsibility (for example, parent, partner, Local Authority, Court Guardian, Special Guardian, etc.)
- Request a positive identification to include a photograph and a signature (for example, passport page, driving License etc.)
- Or compare to earlier material in possession (for example, signed letters).

If there is concern that an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, the response can be sent directly to the individual rather than the third party requestor. The individual may then choose to share the data with the third party after reviewing this.

In some cases an individual may not have the mental capacity to manage their own affairs. There are no specific statutory provisions enabling a third party to exercise subject access rights on such a person's behalf. However, it is reasonable to assume that an attorney with authority to manage the individual's property and affairs, or a person appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority.

5. The right to rectify

6. The right to erasure

5. The right to restrict processing

6. The right to data portability

7. The right to object

8. Rights related to automated decision making & profiling