WARWICKSHIRE COUNTY COUNCIL

Guide for dealing with Subject Access Requests

Data Subject Rights and Access to Personal Information (Subject Access Requests)

Version: 4
Date of issue: June 2017
Review date: April 2018
Reference: WCC-1073-722
Team: Information Management
Protective Marking: Public

Warwickshire County Council

CONTENTS

Page No.

Guide for dealing with Subject Access Requests (SAR)

1. INTRODUCTION

1.1 The Data Protection Act 1998 (DPA) gives data subjects certain rights where organisations' hold and deal with their information.

1.2 This guidance gives an overview of data subjects' rights and our responsibilities. It details one of those rights, that of accessing their own information, known as Subject Access Requests (also known as information access requests or personal information requests). Handling these requests is subject to a legal requirement under Section 7 of the Data Protection Act 1998.

1.3 The guidance shows the procedures that have to be followed and what needs to be considered before releasing information to a data subject.

1.4 On the 1st January 2016 the Council agreed that the Information Management Team will now process all subject access requests made of Children's Services. Adult Services, HR and Education & Learning will continue to process requests made of their services. This includes acknowledging the request, requesting identification documents if not already provided, the processing and disclosure of the requested information.

1.5 All requests regardless of which section deals with them will need to be centrally recorded by Information Management on the corporate MMR (Manage My Request) system.

1.6 The aims of this guidance

- To make staff aware of the process and considerations needed when dealing with subject access requests.
- To assist correct decision making when dealing with access to records requests.
- To advise on the preparation of a file.
- To advise on the process of providing access to records.
- To advise staff on who to contact for advice and guidance.

1.7 Who does this guidance apply to?

This guidance applies to any member of staff of Warwickshire County Council who deals with other peoples' personal information, whether they are:

- Managers and supervisors.
- Practitioners, student practitioners, support, clerical and admin staff.
- Contracted staff including agency, temporary, seconded, and locum staff.

1.8 Why should I read this guidance?

You may be required to provide access to a data subject's personal information which your department holds about them. This guidance aims to support you in completing the process within the prescribed timescale. Importantly, the process of providing access to records is not as simple as just releasing all the information on the data subjects file. The data subject may not always be the focus of the information, there may be information from a third party or you may need to seek consent before releasing some information. You have to consider the source of the information and if we owe a duty of confidence to another person. If we do not comply with the Data Protection Act as an organisation we could face monetary penalties from the Information Commissioner's Office (ICO).

2. LEGAL FRAMEWORK

2.1 The Data Protection Act 1998 covers computerised and manual records of living individuals.

2.2 The ICO provides guidance on subject access requests concerning requests where references, negotiations, managing forecasts or management planning information is involved.

2.3 The Data Protection (Subject Access Modification) (Social Work) Order 2000 provides that personal information held for the purpose of social work is exempt from the right to access, where disclosure to the data subject would be likely to prejudice the carrying out of social work function, by being likely to cause serious harm to the physical or mental health or condition of the data subject or another person. *(See Section 9.11)*

2.4 The Data Protection (Subject Access Modification) Order 2000 provides a similar exemption for Education information which covers personal education information. The (Miscellaneous Subject Access Exemptions) and (Amendment) Order 2000 maintains the existing exemptions within separate legislation covering disclosure of records for adoption; parental order records and reports and special needs statements.

2.5 The Duty of Confidence is a duty established in common law and covers information provided by a member of the public to a health or social care professional. This information should not be disclosed without the permission of the provider, except in circumstances of 'risk of harm'. (*See Confidential and Personal Information Code of Practice (WCCC-1073-67))*.

2.6 **Durant** (2003) is an important case that has implications which need to be considered. The judgment was that the documents he wanted to see were about his complaint, rather than about himself. This complicates the notion of "personal data". The judgment says that even if a person is identified, they are not automatically entitled to see the reference to themselves. To do so, it has to be relatively easy to locate the information, which means in a relevant, structured file: if on a long list of names, or in a system sorted out by some other means than identifying biographical details (for example, names listed or filed by date, not name or address) this wouldn't enable someone to go straight to their details; and they have to be the focus of the information. It's a balancing act again: the person's right to have access to the information depends on the potential impact of the information on the subject (for example, how damaging, or how much it can or has changed their life); and then the extent to which that information focuses attention on a clearly identifiable living individual (some combination of name with one or more of: address, date of birth, other biographical details); and the nature of the related information. If in doubt, consult Legal Services. *(Durant v Financial Services Authority*, *[2003]*. *EWCA Civ 1746)*

3. RIGHTS of DATA SUBJECTS

Personal Data is referred to as information in this guidance. Please refer to the glossary regarding the definition of 'personal data'.

3.1 What data subjects are entitled to:

- Know if we or others on our behalf are processing their personal information.
- A description of the information we hold about them.
- Know why we hold the information.
- Know the source of the information.
- Know who we have given it to.
- An explanation for any decisions made by automated means (such as financial assessments calculated entirely by a computer).
- Require us to correct or erase inaccuracies or irrelevancies in their records and to tell

others we gave the inaccurate information to that it was incorrect.
- Require us to stop processing their personal information if it isn't justified.
- Seek compensation for damage or distress our use of their information might have caused.
- Request a copy of the personal information we hold about them at the time the request was received (subject access requests).
- Appeal to the Information Commissioner or the courts if access is refused or if the legally prescribed timescales for access are exceeded.

3.2 Our responsibilities to protect and assure the data subject's access rights

To protect and assure the data subject's right of access we should:
- Record personal information in a way that promotes people's rights of access and privacy, for example, keeping individual family members' personal information separate.
- Gain consent at the outset to share third party information with those it's about.
- Give them information informing them of their rights.
- Let them know if their records are held jointly (in which case they only need to apply to one organisation) or separately (in which case they would need to apply to each organisation) so they can exercise their right of access to all their personal information.
- Maintain and store records so they can be retrieved when required.
- Locate all of the applicant's identified personal information. If we find we don't hold the applicant's personal information, inform them of that fact.
- Respond.
- Not alter data in any way once a request is received, except for routine recording.
- Provide a full copy of all their personal information they are entitled to with all technical terms explained, when requested.

4. SUBJECT ACCESS REQUESTS

4.1 How often are data subjects allowed to apply for access?

We can refuse a request if we've already complied with an identical or similar request from the same person, unless a reasonable interval has elapsed. A "reasonable interval" depends on:
- the nature of the information,
- why the information is being processed,
- how far we routinely provide a copy of their records to them,
- how often the information or record is amended or added to.

4.2 Data subjects are not entitled to:

- Information if it is likely to prejudice the carrying out of social work function due to the risk of serious harm to the physical or mental health or condition of the subject or someone else.
- Information that in giving it could hinder the prevention or detection of a crime.
- Information that is legally privileged. (Advice/correspondence with WCC solicitors).
- Information in adoption records. *(See Section 4.4)*
- Information provided in confidence. *(See section 9.4)*
- Someone else's information, for example, third party information. *(See section 9.6)*
- Certain information without consent from its source.

4.3 Access rights of children

The right of access extends to children who can understand what it means to exercise that right, (**Fraser Guidelines**) and they can therefore apply for their information as an adult.

4.3.1 Where a child has made a request it is probably sufficient evidence that they do understand, provided we're sure the child has made the request. Where there is doubt, then the current or most recent social worker in the case will be requested to assess the child's understanding of the process and their rights. A record of the assessment and decision should be retained.

4.3.2 Where a parent with Parental Responsibility (PR) wants to access their children's records and the child is of an age that it is considered they would not understand what it means to exercise their rights, then they can access the child's information as long as we are satisfied this is not against the 'best interests' of the child.

4.3.3 However, where their child is of an age to able to understand what it means to exercise their rights, the parent/s should be informed that the child's capability for understanding will be assessed and their consent sought. The child's consent must be gained for the information to be released to their parent. We must also be satisfied that it is then in the child's 'best interests'.

4.3.4 The parent can object to us contacting their child for consent as they may wish to protect their own privacy, in these circumstances we would not be able to disclose the child's information to the parent.

4.3.5 In such cases we must take into account if granting such access would be likely to result in harm or distress to someone, including the child and if so we can refuse access on grounds allowed for in the Subject Access Modification/Social Work Order 2000. (*See section 9.11*)

4.3.6 The social worker assessing the child should provide a summary of their professional assessment, which has been agreed with their manager.

4.3.7 A Guardian ad Litem (GAL) is also entitled, by virtue of their role as officers of the court, to have access to the records of children who are subject to court proceedings.

4.4 Adoption Records

Requests to access adoption records should be forwarded to the Adoption Team, who will deal with the request. Adoption records and reports are exempted by the Data Protection (Miscellaneous Subject Access Exemptions) Order 2000. *(See also sections 2.2 and 9.11)* Individuals cannot use the Act to insist on access to their personal data in those records.

4.5 Access requests from another authority, or by someone other than the data subject

Information requests received from a social worker from another authority are not deemed subject access requests. These requests are an Information Sharing exercise and therefore should be dealt with by the relevant social work team involved.

4.6 Access requests made by an agent on behalf of the subject

Data subjects who can understand their rights of access can appoint an agent to act for them. Agents should provide:

- evidence of their authority to act as an agent
- and confirm their identity and relationship to the data subject in writing
- we must satisfy ourselves that the data subject has without duress, authorised the agent to act for them, but then treat the request as if made by the data subject.

4.6.1 The data subject can specify parts of their records that they don't want their agent to see. A third party might consent to their information being given to the data subject, but not to the data subject's agent. You will need to judge whether it is "reasonable in all the circumstances" to disclose the information without their consent. There is always the option of disclosing that particular information directly to the data subject.

4.6.2 Sometimes people are not able to give written consent for an agent to act on their behalf. We must help them as much as possible to signify their consent, and satisfy ourselves that they have given consent for the agent to act for them.

4.7 Litigation Friend

The role of a litigation friend is to support a child or a protected party (someone who lacks capacity to conduct proceedings) involved in civil court proceedings. A litigation friend can be appointed by the court or accepted by the court, if they can evidence that they can fairly and competently, conduct proceedings on behalf of the child or protected party and show that they have no interest adverse to that of the child or protected party. The litigation friend should be able to provide evidence of their role, either by a copy of the court order or the acceptance of the court for them to act as a litigation friend. The role of a Litigation Friend ceases with the completion of the court case.

4.8 Access requests on behalf of an adult who may lack mental capacity

There is no special provision in the Data Protection Act 1998 in these circumstances. Most will understand what it means to exercise their rights of access, there are however effective, established methods of communicating with people who are lacking capacity.

4.8.1 Clients who lack mental capacity may already have someone appointed to act on their behalf, for example a Lasting Power of Attorney (formerly Enduring Power of Attorney), a Deputy from the Court of Protection, a Mental Capacity Advocate who makes decisions for them or a litigation friend.

4.8.2 The Mental Capacity Act: Code of practice gives advice on how to ascertain if people have mental capacity and if not how to proceed. This can be found on the internet at: https://www.gov.uk/government/publications/mental-capacity-act-code-of-practice

4.9 Access requests to social care records of someone who has died

The Data Protection Act 1998 only applies to the personal information of living individuals, however, when they were alive the people whose information we hold and used, gave it to us on the understanding that we owed them a duty of confidence and good practice. Our public duty of confidence requires us to similarly respect the confidentiality of those who've died as we do that of living individuals.

4.9.1 Equally, there are legitimate interests in the affairs of the deceased person: for example, relatives/next of kin, agents dealing with service charges, executors or administrators of the deceased person's estate and bodies investigating accidents and serious incidents.

4.9.2 It is our policy that access to the social care records of a deceased person depends on the requester's role, their relationship to the deceased person, and the reason for the request.

4.9.3 In all cases the information requested must be relevant and necessary. The authority has the right to deny or restrict access if is felt that disclosure would cause serious harm to the physical or mental health of any other person, or where it would identify a third person.

4.9.4 The decision to disclose or not is based on what would be in the best interests of the deceased person. The deceased person may have placed a restriction or indicated that they did not wish their information to be disclosed, or the record may contain information that the deceased person expected to remain confidential and if this is the case it must remain so.

4.9.5 Under the Access to Health Records Act 1990, the Local Health Authority is responsible for dealing with access to Health Records for deceased individuals.

4.10 Requests from the Coroners Service

The Coroner is required to hold an inquest to determine the cause of death in circumstances where the death was undiagnosed, unnatural, due to violence, during an operation, due to industrial disease or in other suspicious circumstances.

4.10.1 The Coroner is a Public Official, legally acting in the public interest, normally including the deceased and therefore we are usually able to share information where the information is necessary and relevant to their enquiries and therefore access to social care information about the care that the deceased received and our involvement can be relevant.

4.10.2 The usual exemptions apply to third party information and information covered by a duty of confidence to a member of the public.

4.11 Requests from the Police

Disclosures to the Police are not mandatory except in cases where the council is served with a court order requiring information. However, Section 29 of the Data Protection Act 1998 gives statutory powers to the council to release information to the police without the consent of clients or members of staff for the following purposes:

- The request must be due to the prevention or detection of a crime.
- The request must be due to the apprehension or prosecution of a crime.
- Non-disclosure would be likely to prejudice their investigation.
- The request must be due to the assessment or collection of any tax or duty of any imposition of a similar nature.

4.11.1 If you're unsure if the disclosure fits into the above categories, please contact the Information Management Team or Legal Services for further advice.

4.11.2 The police must put their request in writing on their Disclosure Request Form, stating the enactment and detailing the sections (for example: Section 29) they are relying on to request the information. The police officer should complete the form and have it signed by a senior officer. Only information relevant to their enquiry should then be provided.

4.12 Annex C Requests

These requests will be passed to the MASH Team, their email address is: mash@warwickshire.gcsx.gov.uk

5. SUBJECT ACCESS REQUEST – APPLICATION PROCESS

5.1 People who are currently receiving or have recently been receiving a service may ask to see a particular assessment of them or a report to find out why a particular decision was made. In these instances these requests will be treated as 'business as usual' and responded to in line with our open access policy, recording what has been provided.

5.2 Where individuals are asking to see information unrelated to a current ongoing issue or who are asking for everything we have about them, these would be classed as official subject access requests. The Data Protection Act 1998 clarifies that a verified request to access an individual's personal information is when:

- the request is received in writing (emails are acceptable) – these may described in various ways, for example, information access requests, a Freedom of Information request, a request for personal information, or I wish to see my files.
- we are satisfied of the requester's identity and
- of their right of access.

5.3 Members of the public wishing to request access to their personal information can apply using the Personal Information request - online form via our website link at: http://www.warwickshire.gov.uk/dataprotectionact as this links directly into the Corporate MMR system for logging and monitoring requests for access to information. This site also provides details of alternative ways to make requests

5.4 When you receive a new request you will need to pass to the Information Management Team as soon as possible for logging and processing, this should include the date that you received the request and the nature of the request, for example, a request for a deceased person's records, a Continuing Health Care Review request, an individual requesting their information or an employee requesting their personnel records. It is helpful if you are then able to provide confirmation of the requester's identity and details of any significant concerns or issues that may impact on the processing of the request.

5.5 On receiving a new request the Information Management Team will log the request on the Corporate MMR system. This will enable clear management of the request with an audit trail and reporting functions. All the administration of the request process will then be carried out through the MMR system.

5.6 Where the identity of the requester cannot be verified by a relevant worker for example a social worker, we will require two forms of evidence from the requester; this will normally consist of one of each of the following; (we do not accept birth certificates as proof of identity).

Photographic

- Passport
- Driving License
- Citizen Card

Address

- Bank Statement
- Council Tax bill
- Utility Bill

5.7 All requests must be acknowledged as soon as possible, where the requester's identity has not been verified, this can be requested in the acknowledgement. The request is not valid until the evidence is received and we are satisfied of the requester's identity and their right of access; from the date of receipt of the evidence we have 40 calendar days to complete the request. Where further clarification of the request is required the 40 calendar days does not start until receipt of that clarification.

5.8 The Data Protection Act 1998 allows a fee of £10 to be charged for this service, at present Warwickshire County Council does not charge the permitted fee. Education records are held by schools who can charge upto a maximum of £50.

5.9 The Information Management Team is available to provide advice and guidance on this subject.

6. SUPPORT OF STAFF PROCESSING REQUESTS FOR PERSONAL INFORMATION

Those supporting staff through the process should:

- Recognise the work can be time-consuming and give staff concerned time to carry it out.
- Supervise and monitor case recording to meet appropriate standards of both open access and third party confidentiality.
- Ensure staff understand information governance, in particular data protection, confidentiality and data subject rights; and the process and standards for complying with subject access requests in Warwickshire.
- Ensure that staff processing, understand the status of: supervision notes; emails; third party information and sources; restricted information; and record and file accordingly.
- Help staff to be clear about the specifics of the request, so they understand the scope of the redaction exercise.
- In complex cases or where staff are inexperienced, carry out/share the redaction personally.
- Allocate admin time for copying records, calling in sub-files and transcribing when required.
- Prioritise staff workloads to help them complete subject access requests timely.
- Advise staff on obtaining legal and other expert advice, as needed, especially in complex, sensitive or difficult cases.
- Progress-chase requests for information ensuring timely and appropriate responses are given.
- Alert senior managers and those with Information Governance responsibilities if there are compliance difficulties.
- Take any issues and lessons learned and turn them into staff development opportunities.

7. LOCATING THE FILES

7.1 Check exactly what information has been requested. You need to be very clear about what's being asked, and where relevant information might be.

7.2 As more partnership working takes place, remember that information could be held on more than one agency. So you need to consider the following:

- Which specialist workers, teams and units have been involved with the requester,
- What records exist in archive, on-site and off-site storage,
- Downloading a copy of electronic records from relevant data system e.g. Mosaic / CareFirst.

7.3 Once you have identified, located and called in all other relevant files and records, you are now ready to have the paper files photocopied or where applicable, scanned into a ‘pdf’ format *(Portable Digital Format)*.

7.4 Once the copying or scanning of all the records has been completed these will form your ‘original copy’ of the requested information and if in an electronic format should be held in a confidential folder named ‘Original Information’.

8. PREPARING AND REDACTING THE INFORMATION

8.1 For preparing and processing information using Adobe Professional software please refer to Appendix 2

8.2 For preparing and the manual processing of information please refer to Appendix 3

9. CONSIDERATIONS FOR WITHHOLDING INFORMATION:

9.1 There are a number of reasons for withholding information from a data subject, these are:

- Third Party Information (personal information about someone else).
- Information provided in confidence.
- Legally privileged (advice/correspondence between staff and WCC solicitors).
- Waiting on third party consent
- Court Documents
- Data Protection (Subject Access Modification)(Social Work) Order 2000. *(See Section 9.10)*

9.2 If it is clear the data subject is already aware of the information there is no need to withhold it, but be careful of instances where the data subject may know about the information, they may not know that another organisation has passed this information onto the council.

9.3 Do seek advice if unsure as this is not an exact science, you often have to risk assess finely balanced rights and issues.

9.4 Duty of Confidence

A duty of confidence arises between a member of the public and a professional where one party has information relating to another party in circumstances giving rise to an expectation that it remains confidential. Some examples are; a doctor has information about patients; a solicitor has information about clients; an employer has information about employees or a social care worker has information about service users provided by third party. If a clear duty of confidence arises, disclosure without third party consent is unlikely to be reasonable.

9.5 How to Deal with Consents for Disclosure

9.5.1 As of April 2016 it has been decided that in the interests of expediency in the turnaround of Access Requests the Information Management Team will not seek to gain consents from third parties including Health professionals, the information will be reviewed in line with the guidance and disclosed where decisions are that it is appropriate to disclose (case by case basis).

9.5.2 Police Data

Generally information provided by the police which directly relates to the data subject's personal history or information relating to a potential criminal investigation will be withheld as 'Third Party Information/Police Information'; however you will need to review the identified information to consider if disclosure is appropriate.

9.5.3 Where it has been decided that a request for consent to disclose third party information should be sought, it should be done as early as possible as they can take time to obtain. You will need to copy it and send it with a covering letter to the source, with a date required for return. Remember you may still have to redact any information not relevant for the recipient to see and remember to keep a copy of what you have sent.

9.6 Third Party Information

Third party information is information about someone other than the data subject. It would include references to their family and friends, other non-Council professionals and agencies, consideration would need to be given if this information should be released.

9.6.1 Information provided by someone else is not the same thing, for example people who have referred concerns about the data subject, these could be relatives, or non-council professionals or agencies acting in their professional capacity, consideration would need to be given if this information should be released.

9.6.2 For information provided by a member of the public/relative this is generally considered as provided in confidence and as such would be withheld.

9.6.3 Legally Privileged Information

Legally privileged information is exempt from disclosure to the data subject where it is professional legal advice is being sought from and being given by the Warwickshire County Council's Legal Governance Team in respect of the service to the data subject.

9.7 Information about our own staff

Our own staff are deemed to be "relevant persons" when acting in their official capacity (this includes foster carers and others employed as agents for social care teams). Staff acting in their personal capacity are third parties. The distinction is important as references to them in their official capacity may only be removed if there is clear risk of harm to someone; you don't need their consent to disclose the information referring to them.

9.7.1 There is another consideration: that of staff whose reference in someone else's information is clearly incidental.

Example 1:

An Admin Assistant's name features on correspondence just because they typed and distributed the minutes as their role in administrative processes was incidental; it has no impact on or part in the personal information. Their name can be withheld, though you would leave in the reference to "Admin Assistant".

Example 2:

Suppose a data subject phones to speak to the manager or a practitioner, but speaks to an Admin Assistant in their absence. The Admin worker agrees to record and forward the details to the relevant worker. The data subject subsequently complains that the worker didn't contact them afterwards, and the worker claims they did not get the message. The Admin Assistant's role in a complaint investigation then becomes key as their identity would have been given to the data subject during their conversation. In this case, you would not withhold their name.

9.8 Can people see supervision notes about themselves?

Yes. Personal information about service users contained in supervision notes is no different from any other personal information.

9.81 Where the notes focus is on the worker's performance, staff care needs or personal and professional development; and any personal references to the service user are incidental, you can withhold the supervision notes, as their focus is the workers personal information.

9.82 Where the focus is on what has happened so far in a case, plans for the future and any professional views about the circumstances of the individual or family; then unless you can justify withholding the information, people are entitled to see what is in those notes.

9.83 It's a fairly common misunderstanding that supervision notes are confidential, restricted from the people they are written about, that their focus is the worker's work etc.

9.84 You can withhold the relevant information in the supervision notes for a time if the case is sensitive, there are conflicting interests, risk of harm etc., but once the risk is past, conflicting interests reconciled or managed, the information would then be accessible.

9.9 Information from Health Professionals

This applies to personal information about the physical or mental health or condition of the data subject. Where correspondence from health professionals and agencies is stamped confidential, this context usually means "it contains sensitive, personal information and must be transmitted and kept with appropriate care", it doesn't necessarily mean it is restricted from the data subject.

9.9.1 As of May 2016 the Information Management Team will disclose general health information that has been provided by health professionals and which is known by the data subject. Information held within specialist health reports for example Psychology Assessment Reports, will not be disclosed and the data subject will be directed to the responsible Health Service.

9.9.2 Increasingly, health professionals do copy patients into correspondence at the time about their health. Where it is evident that the data subject has already had, or knows the information in question you are not required to provide it again, unless you believe they have lost/forgotten it and you are concerned about its renewed impact on them; for example, could there be a risk of harm to someone? In these cases the information should be withheld.

9.10 Information from other professionals and agencies

The default for any information we handle, including any that other professionals/agencies give us apart from health information, should be to disclose it to data subjects. This is because information about the data subject they have provided may often represent that professional's opinion and as such could be released unless any other exemptions apply. Staff are not always aware of this and staff receiving information from other agencies should remind them of this approach.

9.10.1 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.

9.11 Data Protection (Subject Access Modification) (Social Work) Order 2000

This enables consideration for withholding information if it is likely to prejudice the carrying out of social work by causing serious harm to the physical, mental health or condition of the data subject or another person. The use of this exemption should be exceptional and confined to serious harm. The order confirms that the identity of social workers as relevant people should be disclosed but also confirms that this can be overruled if the serious harm test applies.

9.12 What is reasonable to disclose, how do I know if I can disclose it or not?
The Data Protection Act does not provide any guidance on what is reasonable in all circumstances and there is limited general law giving guidance on this specific issue.

9.12.1 There can be conflict between a data subjects right of access and a third party right to privacy. You have to balance the rights of the various individuals and it is our decision whether information can be released where you feel it is reasonable in all the circumstances to do so.

9.12.2 Where responding to the request may disclose information about another individual (a third party), who could then be identified from that information, you are not obliged to disclose it as we have a duty not to breach confidence. However, you may decide that it is reasonable to disclose the information, for example where the third party has contributed to a record in their professional capacity. These decisions should always be taken on a case by case basis, after careful consideration and in the light of the relevant circumstance surrounding each case.

9.12.3 Where a clear duty of confidence arises, disclosure without third party consent is unlikely to be reasonable unless the disclosure would fall within legally recognised exceptions or is clearly in the public interest.

9.12.4 Where there is no duty of confidence, it maybe reasonable to disclose third party information, unless the information is sensitive, or where it is likely to cause harm.

9.12.5 If the decision is that it is **not** reasonable to disclose third party information you need to consider if some information could be disclosed without breaking confidentiality. For example removing the third party identity or redacting the document. If in doubt, consult Legal Services.

9.12.6 Considerations when making decisions regarding the treatment of third party information are:

- Do we owe a duty of confidence to the third party whose personal information we are considering disclosing?
- What does the subject already know or is likely to find out? If they already know this information, we aren't disclosing it.
- Is the third party information confidential, sensitive or harmful?
- Was the source "a relevant person"? Only the likelihood of serious harm would suffice to exempt the information from access.
- Can it be edited to protect the third party's identity appropriately?

Ultimately the information would be withheld if:

- It's not clear that it's reasonable to disclose the information without it; and
- Information can't be edited appropriately removing identifying references to a third party.

9.13 Information held on e-mails:
Emails are no different to any other record containing information and should be retained as part of the permanent record. Corporate ICT periodically require us to delete inconsequential and personal e-mails.

9.13.1 But: all emails containing personal information about people in connection with the work of the council (whether recipients of services; those referring, their family and friends; workers; other professionals and agents); and emails that affect council business (that record decision-making, policy, advice) should be retained as part of a permanent record whether in electronic or hard copy form, for the duration of its operational life (until the prescribed destruction date). To destroy or mislay them is in breach of the law.

9.14 'Restricted' information on file

Restricted information generally by its very nature means there are reasons to withhold the information. As time elapses the information may no longer be restricted and there may not be any reason to withhold this information, consideration should then be given to whether it can then be released. For example: Minutes of closed sections of Child Protection Conferences or Safeguarding minutes.

10. ONCE REDACTION IS COMPLETE.

10.1 The redacted information can now be provided to the requestor along with a covering letter explaining the exemptions you have used where relevant the Information Management Team can provide suggested letters if needed. By default, the Information Management Team provides the redacted information to the requester using secure email (Egress). For manually redacted files these will need to be photocopied and sent out to the requestor with a covering letter. It must be posted securely, in line with the Information Handling and Security policy.

10.2 If the effort to print the records is disproportionate, access can be provided in different ways;

- Provide the information in an electronic format using a secure email facility (Egress).
- Do a summary and/or print any documents the subject specifically wants.
- Go through it verbally with them from the original files (however there are issues about protecting other people's information),

10.3 Where files are to be provided verbally, it is important to obtain the subject's agreement to this and to get them to sign and date to confirm they have seen the records and when, also why any information has been withheld from them. Overall this method is not advisable as providing documents, has more credibility especially in complaint cases and also due to the issue of protecting third party information. If they insist on a full copy, it is their right, so if you still think the effort to copy it and edit it for third party and exempt information is disproportionate, seek legal advice.

10.4 However, some people will want support when going through their records for what can sometimes be painful and distressing information and therefore may wish to have a companion or an advocate to support them. Individual circumstances will determine how and where access should be arranged.

10.5 We do not have to make disproportionate efforts to provide access, so you can to that extent choose the option. Arranging to see people to explain their records and answer their queries takes longer than just sending a copy but we do need to take into account, and be sensitive to, the person's circumstances and preferences too, to ensure their access to their personal information is as constructive and helpful an experience as possible.

10.6 The data subject has a right to appeal against our refusal to give access, which they obviously can't exercise if they don't know an exemption exists. Therefore, it is good practice to make notes relating to how you reached your disclosure the decisions about the withholding of information and notes on any exemptions you relied on. For manual redactions this would form the schedule. The Information Commissioner (ICO) could ask the department to explain and justify its actions and decisions following a complaint by an individual.

10.7 Remember people are entitled to challenge whether we have complied with our DPA duties properly so it is important to have exact copies for future reference, should they complain.

10.8 People whose first language is other than English, or/and blind or/and partially sighted, will need information either translated or made available in different media.

10.9 Finally inform Information Management of the date the request was completed along with the time spent preparing and processing the request, also the number pages that have been dealt with. This is then recorded on MMR for reporting purposes and the case is then closed.

11. FOLLOWING DISCLOSURE OF A SUBJECT ACCESS REQUEST

11.1 People have certain rights they might wish to exercise as a result of access to their personal information. They can:

- Ask us to stop processing their information, if they think it will cause them unwarranted, substantial damage or distress.
- Seek compensation if they think we have breached the law.
- Ask us to correct or erase inaccurate or unnecessary information.
- Ask us to rectify it with anyone we gave the wrong information to.
- Ask for an Internal Review of the disclosed information *(See section 11.4)*
- Complain to our Customer Relations Team if unhappy with the way we handled their request; and/or the Information Commissioner if they wish to appeal against our decision on access or appeal to the courts.

11.2 Corrections/Amendments to Records

People have the right to ask us to correct or erase inaccurate or unnecessary information:

- If we do not agree that the information is inaccurate, we should note in the record that the subject regards the information as inaccurate.
- It is good practice to deal promptly with requests for data to be corrected in order to avoid potential court action or intervention by the Information Commissioner.
- We should send a copy of the corrected data to the subject if applicable.
- If we have made amendments to the record we should also provide this to anyone we have given the incorrect information to.
- If the request isn't appropriate, it should be explained why we can't action their request.

11.3 Although the Data Protection Act does not set any timescale for us to respond to such requests, we should aim to inform data subjects of the action taken within 21 days of receiving the request. *(As recommended in the Departments of Health's Guidance for Social Services on the Data Protection Act 1998.)*

11.4 Internal Review

Once the request has been completed and closed, if the requestor is not satisfied with how the request has been dealt with, they do have a right to go directly to the ICO. The requestor can also ask us for an Internal Review (the ICO will not deal with their request unless they have gone through an Internal Review first). They need to request an internal review within 40 days of receiving our response by writing to the Information Management Team with details of why they are unhappy with the processing of their request. Legal Services will deal with any Internal Reviews and the process can be managed through the MMR system. If you do not have access to MMR, inform the Information Management team who will log the review request on the system which will then be allocated to Legal Services.

12. HOW TO AVOID COMPLAINTS ABOUT SUBJECT ACCESS REQUESTS

12.1 People under stress, who aren't familiar with the law, or who don't possess confident writing skills, will not always express themselves clearly or tactfully, So read the requests carefully as getting it right early can save a lot of difficulty and time later on.

12.2 Clarify with them if necessary until you and they have a clear understanding of what is being requested as they may not want everything. They may just want something specific.

12.3 You won't always be able to respond in full in the timescale (40 calendar days), though you should always try to and meeting the request in full within 40 calendar days should be the norm.

12.4 What aggravates people more than anything, however, isn't necessarily that we can't provide everything within that timescale: but that we don't keep them informed. So it is important to keep them informed of progress and to inform them if there is to be a delay.

12.5 Where you have decided to seek consent to disclose third party, you should do this as early as possible as they may take time to obtain (although this should not delay sending out the main bulk of the information).

12.6 Provide as much information as you can within the 40 days, with an indication of when you hope to provide the rest. If you are unable to keep to that, let people know you can't, and why.

13. GLOSSARY OF TERMS

Data Subject: the person the information is about.

Personal data: information which relates to a living individual who can be identified (in other words, just because their name isn't mentioned, this doesn't make it less relevant, if the context or other details clearly identify them). If in doubt, consult Legal Services.

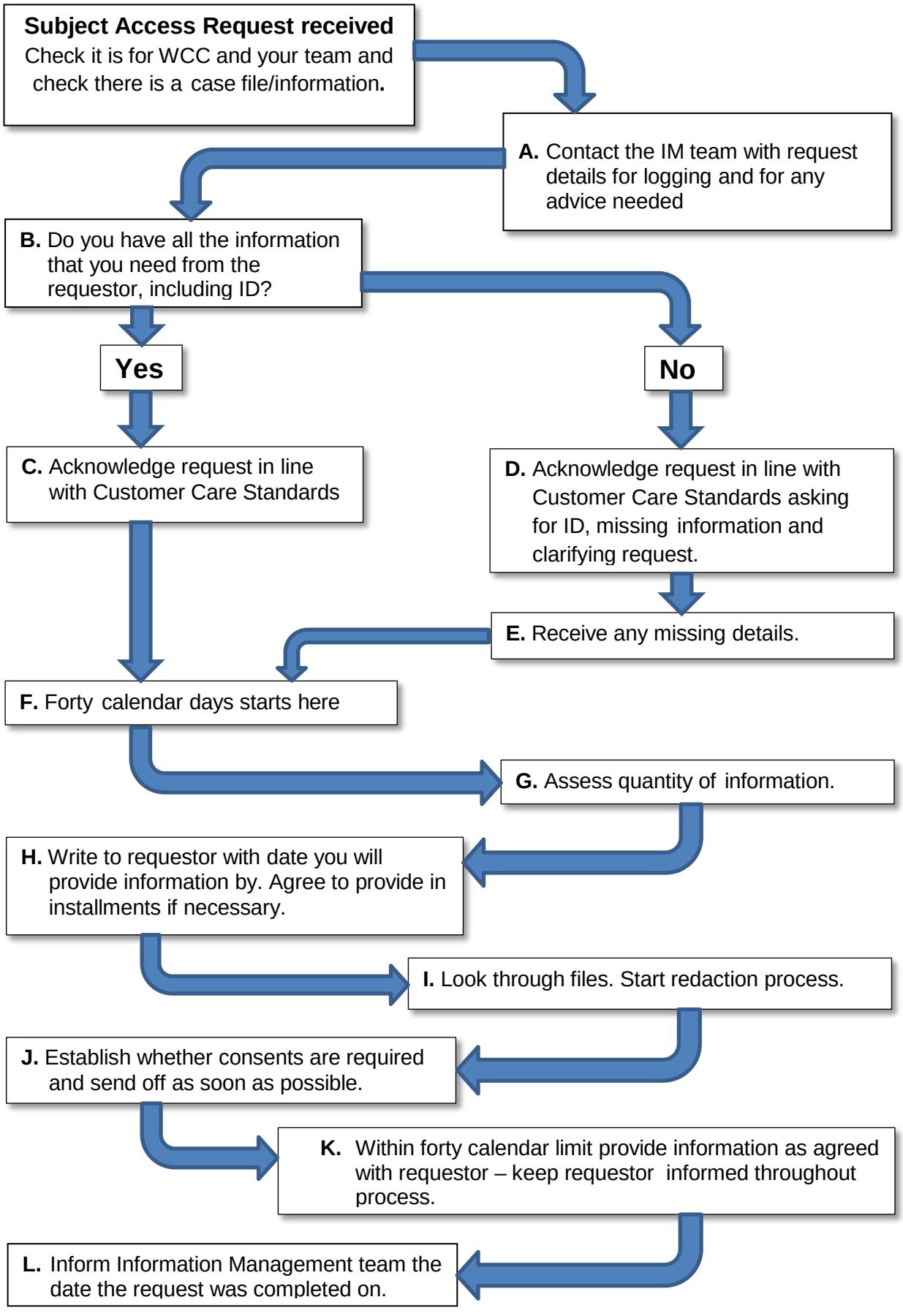
Proportionality: balancing the effort of collecting information against the impact on the subject of giving or withholding the information.

Third Party: someone else mentioned or referred to in the information, other than the subject.

Source: the person who gave the information.

Relevant person: The Data Protection (Subject Access Modification)(Social Work) Order 2000 doesn't allow us to refuse access on the grounds that someone else would be identified, if they were a "relevant person" for example, a social worker or foster carer, unless the serious harm test applies.

APPENDIX 1 – FLOWCHART - DEALING WITH REQUESTS FOR PERSONAL AND CONFIDENTIAL INFORMATION



Additional Notes to Flow Chart

A. Inform the Information Management Team of the request and the date it was received. The Information Management Team can also:
- Provide you with advice and guidance through all stages of the process,
- Offer face to face mentoring.
- Check through documents you are unsure of.

B. What has the requestor supplied:
- Ensure the request is in writing (unless circumstances mean it is not possible for the person to apply in writing).
- Has proof of identity been supplied, when required.
- Ensure we have a form of authority if someone is acting on the data subjects' behalf.

C. If the request is valid then send an acknowledgement in line with the Customer Care Standards with details of expected date of completion. Go to point **F**.

D. If clarification of the request, identification or more information is needed before proceeding then send an acknowledgement asking:
- Proof of identity and residence – to ensure they are entitled to receive the information.
- What information are they particularly interested in?
- Whether there is any particular time period, incident or decision that they would like to know more about?
- Whether there are any specific documents or types of documents i.e. case conference minutes they are interested in?
- **Note** - The requestor is entitled to see **all** their personal information if they wish and they do not have to provide a reason why they want access.

E. Received the requested missing information, the request is now valid. Go to **F**.

F. Forty calendar days is the statutory timescale to respond under the Data Protection Act 1998. This only starts once you have verified and have sufficient information to make a start. Ensure the requestor knows who to contact with any queries they might have.

G. If it is impossible to meet the statutory timescale you must at least provide some of the information by that date and you must provide a reasonable timescale for what is outstanding.

H. Keep them informed of progress especially of any delays. If we fail to respond timely and appropriately they can complain to the Information Commissioner.

I. Start the process of redaction (deciding what to leave in and take out).

J. Requesting consents should not hold up the process. Other information can be released with a letter to the requestor explaining that we are still waiting for permission from a third party to release some information.

K. Provide information available within the 40 calendar days if possible.

L. Inform the Information Management team the date the request was completed on.

APPENDIX 2 – PREPARING AND REDACTING INFORMATION USING PROFESSIONAL SOFTWARE

1. This section provides further guidance for the processing of personal information using professional software.

2. **Redaction** is the process of going through case files and preparing the information for release to a data subject.

3. All of the requested personal information files which are to be processed should be held in a **confidential** named folder (data subject's reference) with restricted access as necessary. These scanned and downloaded files should each have a unique file name to ensure that particular pieces of information can be easily located should the need arise.

4. Within the confidential folder, there should be two sub-folders, one named **Original Information** and one named **Working Information**. A complete copy of the personal information held in the Original Information folder can be taken and placed in the 'Working Information' folder, these documents are now your working copies ready for redacting.

5. Processing now requires you to go through the working copy, page by page and decide what information:

- Can be disclosed,
- Has to be withheld,
- You need to get consent to share,
- You are not sure about (flag these to come back to so you can make a decision later).

6. Using the software on your working files mark for **r**edaction the information you have decided that is not to be disclosed to the data subject. Each redaction mark will need to have a note added in the top left hand corner where possible, giving the reason why the information has been removed, for example: 'Third Party Information' or 'Legally Privileged Information'.

7. In large or complex cases you will need to create a rationale document which provides details of the decisions you have made in marking the information for redaction. This would prove invaluable where there is a need for a review of the request.

8. Where possible you will need to transcribe information that would otherwise be difficult for the data subject/requester to read.

9. Once you have completed reviewing all of the information, the redaction marks can be applied. Each file should have a footer providing the following; in the left – 'Data Subjects Copy'; in the center – the 'page number' and the 'number of pages' and in the right – the 'icasework'(MMR) reference number.

10. For reference, once you have finished redacting the file you should have the following: -

- A copy of the original request.
- Any other relevant correspondence including consent information.
- Original copy of the files. (copy number 1)
- Your redacted working copy of the files. (copy number 2)
- A rationale of notes on the decisions you have made.

APPENDIX 3 – PREPARING AND REDACTING INFORMATION MANUALLY

1. This section provides further guidance for the preparation and manual processing of personal information.

2. **Redaction** is the process of going through case files and preparing the information for release to a data subject.

3. Manual redaction should be carried out by members of staff that have knowledge of the records, preferably the person who writes the information and can determine what should be exempt. But in more complicated, more substantial, or more contentious requests, where there might be conflict of interest, sensitive third party information, questions of whether to restrict certain information etc., line managers should support the staff member concerned. The Information Management Team can be contacted for further advice and support.

4. Where a member of staff delegates the task to others, they should give specific instructions about what to include or exclude.

5. The process of manually redacting a file is likely to be a big task and you will need to take account of the following points as a guide to assist you in completing the preparation of the information for release to the requester. You should also ask for administrative help if needed.

6. Make sure you have numbered the original files, this enables you to double check everything has been photocopied and means it's easier to refer to if you later receive a query regarding the redaction. You can then take a photocopy of the files or the specific documents depending on what has been asked for; this will then be your original copy (copy number 1). Make a further copy of this information; this will be your working copy (copy number 2).

7. On your working copy (2) remove (redact) the information that is not to be disclosed. You can do this in a number of ways, depending on what you have to remove: there is specialist cover-up tape, tippex, marker pen, post-it notes. Make sure that no non-disclosable information shows through.

8. You will need to either note on the page itself where the information has been removed and why, or create a schedule referencing page number, type of document, date and reason why it has been wholly or partly removed.

9. The data subject has a right to appeal against our refusal to give access, which they obviously can't exercise if they don't know an exemption exists. It is good practice to make notes relating to how you reached your disclosure and withheld information decisions and notes on any exemptions you relied on. The Information Commissioner (ICO) can ask the Council to explain and justify its actions and decisions following a complaint by a requestor.

10. Throughout the documents where possible transcribe information that would otherwise be difficult for people to read.

11. You then photocopy your completed (redacted) working copy (2) for sending out to the requestor (copy number 3) along with the schedule explaining the exemptions you have applied, if relevant.

12. Please double check the requester's copy (3) for any redacted information that may be visible, if so you will need to rework to ensure that redacted information is not disclosed. Do not send the original working copy (2), this is to avoid people washing out marker pen blocking, or scratching off tippex, and seeing information they are not entitled to see.

13. You should then be left with the original copy (1) of the file and your original working copy (2) and the schedule if applicable.

14. For reference, once you have finished redacting the file you should have the following: -

- A copy of the original request.
- Any other relevant correspondence including consent information.
- Original copy of the files. (copy number 1)
- Your redacted working copy of the files. (copy number 2)
- Any notes you have on decisions made for your records.
- A photocopy of the redacted working copy for release to the requestor. (copy number 3)
- Where applicable a copy of the schedule for the requestor and a copy for your records.