Subject Access Request Procedure

Altogether better

Durham County Council

Details:

Review Frequency: Every 3 years	Date of last review: May 2018	Date of next review: May 20121
Service number ID (if appropriate)	Manual: Information Management (Transformation and Partnerships)	

Version Date	Version ref	Revision History	Reviser	Approved by	Review Date
Oct 2014	Version 10	Final			
May 2018	Version 11	Draft	Paula Sheen		
Jun 2018	Version 12	Draft	Lawrence Serewicz		

Contents

Summary/Introduction

1. Durham County Council processes large amounts of personal information to deliver services to its customers. These customers have a right under the EU General Data Protection Regulation (GDPR) to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing of their data. This right is called the right of Subject Access. To meet that legal obligation, the council has a procedure to respond to Subject Access Requests (SARs).

2. This procedure sets out the process for dealing with requests for personal information as governed by the GDPR and the Data Protection Act 2018 (DPA18). It covers the decision making process used to decide whether the information should be released.

Purpose

3. This procedure is designed for Durham County Council employees to help them respond to subject access requests made by an individual (the data subject) or by someone (a third party) on the individual's behalf. The procedure covers Subject Access Requests under the GDPR, the DPA18 and the Access to Health Records Act, which covers the medical records of the deceased.

When the council decides to disclose information, it has to consider legal issues relating to privacy and confidentiality. This e procedure is to help you provide a response and comply with the relevant legislation. The procedure covers the principles of handling a request and it is not a definitive procedure to cover every eventuality. All requests are different and need to be considered on a case by case basis.

The Information Management Team can be contacted at any time for advice and guidance on either 03000 268034 or at dataprotection@durham.gov.uk

Scope

4. This policy applies to all personal and special category data held by Durham County Council in any format.

Definitions

Data	A collection of facts from which conclusions may be drawn
Personal data **(as defined by the GDPR)**	**Personal Data** - any information related to a natural person or 'Data Subject', that can be used to directly or indirectly to identify the person. In practice, these also include all data which are, or can be assigned to a person in any kind of way. For example ▪ Name ▪ address ▪ telephone number ▪ credit card ▪ personnel number of a person ▪ account data ▪ appearance ▪ location data such as IP address
Special Category Data **(as defined by the GDPR)**	**Special category data** is any personal information that is one or more of following categories: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious or philosophical beliefs ▪ Trade union membership ▪ Genetic data (new) ▪ Biometric data (new) ▪ Health Data ▪ Sexual life
Data Protection Principles (as defined by GDPR)	There are 6 data protection principles as follows: 1. **Lawfulness, fairness and transparency** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject **2. Purpose Limitation** Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes **3. Data Minimisation**

	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. **4. Accuracy** Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. **5. Storage limitation** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with Article 89(1), subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject. **6. Integrity and Confidentiality** Personal data shall be processed in a manner that ensures appropriate security of and, against accidental loss, destruction or damage, using appropriate technical or organisational measures
Lawful Basis for Processing **(as defined by GDPR)**	Personal data shall be processed lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Article 6 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Article 9 is also met. The conditions for processing are set out in Article 6 and Article 9 of the GDPR (Appendix 2), unless a relevant exemption applies.

Legal Context

5. The GDPR and the DPA18 regulates the processing (use) of information relating to living individuals, including the obtaining, holding, destroying or disclosing of this data.

6. Any request for information relating to adoption is specifically dealt with under the Adoption and Children Act 2002. Any such requests should be forwarded directly to the Fostering and Adoption Team to handle adoption@durham.gov.uk

7. Any disclosure under the Access to Health Records Act requires a medical professional to be consulted on the disclosure. Only medical professionals can order a disclosure under this Act.

8. An individual is only entitled to their own personal data and not to information relating to other people (unless the information is also about them or they are action on behalf of somebody else).

9. The specific right to access of personal data under the GDPR is found in Article 15. The data subject has the right to be informed whether their data is being processed and where that is the case to access that personal data and the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

10. Where a request is made electronically, the information should be provided in a commonly-used electronic form, unless otherwise requested by the individual.

11. The information must be provided free of charge however when a request is manifestly unfounded or excessive, particularly if it is repetitive, a reasonable fee can be charged based on the administrative cost of providing the information.

12. Information must be provided without delay and at the latest within one month of receipt of the request and evidence of identification. This can be extended by a further two months where requests are complex or numerous. If this is the case, the individual should be informed within one month of the receipt of the request together with an explanation as to why the extension is necessary. To enable the deadline to be met, services need to provide the information 10 days before the deadline to enable redactions to be made and for the response to be prepared.

13. The right of subject access is a broad and powerful right. It covers any and all information held by the council that is classed as the applicant's personal data. To comply with this right, the council must review any and all documents containing the data subject's personal information for possible disclosure. There are no exceptions to this requirement. The Act overrides any duty of confidence, or any other laws such as employment laws around disciplinary files. If the council fails to consider a document for disclosure, then there can be a criminal charge as it is an offence under s.77 of the Freedom of Information Act (FOIA) to withhold information without authorisation that an applicant is entitled to receive.

14. Please note that all documents must be considered **before** the council can decide whether to disclose the documents.

15. The Access to Health Records Act 1990 was mostly superseded by the Data Protection Act however it still allows for the records of deceased data subjects to be accessed by their representatives or anyone who has a claim arising as a result of their death. Please note that medical records can only be disclosed on order of a medical professional and social care records are not medical records.

Subject Access Requests

Roles and Responsibilities

Members

All elected members are to be made fully aware of this policy and of their duties and responsibilities to safeguard confidentiality. Members are also bound by the Members' Code of Conduct and are their own data controllers for any case work linked to their duties.

Staff

All staff will be required to observe this procedure and be aware of the rights of service users to request access to their records in order to safeguard confidentiality and preserving information security.

Corporate Management Team (CMT)

CMT has overall responsibility for ensuring that staff comply with the Councils legal obligations regarding the handling of personal information and for the development of any service specific guidance for sharing of information**.**

Senior Managers

Senior Managers are responsible for ensuring that all staff are compliant with the requirements of the policy and that confidentiality and for advising, dealing with and monitoring any issues regarding disclosure or access to information.

Team Managers

All Team Managers must ensure that they know and understand this procedure and all related organisational procedures for access to personal records. They must be aware of the need to conform to these procedures and the actions agreed for sharing information. They are also responsible for ensuring their staff are aware of the requirements and should be the first point of contact for staff for the provision of advice and support on confidentiality issues.

Information Management Team (IMT)

The IMT based in Transformation and Partnerships provides the Data Protection liaison for the Council and will provide advice, guidance and support in relation to confidentiality and Data Protection issues. The IMT log and co-ordinate all subject access requests for the council

Legal Services

Legal services will provide advice and guidance on legal issues to the Information Management Team – services should not seek legal advice direct without first consulting IMT.

Data Protection Officer (DPO)
A DPO is a statutory role as the legislation requires qualifying public authorities to have one. The DPO is an expert in data protection who monitors internal compliance; informs and advises the council on its data protection obligations; provides advice regarding Data Protection Impact Assessments (DPIAs); and acts as a contact point for data subjects and the supervisory authority.

The Data Protection Officer in Durham County Council is:
Roger Goodes
Head of Communication and Information Management
03000 268050

Receiving a request

16. Anyone can make a subject access request. For a request to be valid, it must meet the following requirements:

- The request can be made by letter, electronically, or verbally and can be made to any part of the organisation. Where the request is made verbally, the details of the request must be recorded by the receiving officer.
- The data controller (the council) must be satisfied as to applicant's identity. In some cases this will be a copy of a photo id and a signature, in other cases, where the applicant is well known to the service, this may not be required. Please note that some services such as Revenue and Benefits may have specific checks that have to be completed before the personal data can be released.
- Where we process a large amount of information about an individual we can ask them for more information to clarify their request. You should only ask for information that you reasonably need to find the personal data covered by the request. If they refuse to provide the information, the request should still be accepted

17. We recommend that an applicant uses the DCC portal or the Subject Access Request form (Appendix 1) which are available on our internet site. However, any written or verbal request can be accepted.

18. All requests should be forwarded to the IMT for logging. The IMT will acknowledge the request and where the request has been made verbally, they will include a copy of the request. This will help avoid any later disputes about the information that has been requested

19. Please note that there is an important difference between Business As Usual (BAU) requests and a Subject Access Request (SAR). A BAU request for personal data is like asking for your bank balance. A SAR is like asking for all the personal data the bank holds about you. In most services, there will be

procedures in place for a person to find out about their account, such as finding out their council tax bill or checking on the status of a service request. These are not subject access requests even though they are receiving their personal data. A SAR needs to be logged with the Information Management Team (IMT) a BAU does not.

Charging for copies of records

20. The Data Protection Act states that records should be provided free of charge however where a request is manifestly unreasonable or repetitive, e.g. repeated requests for the same information, an administrative charge can be made. This will be in accordance with the EIR/SAR charging policy

Timescale to respond

21. There is a statutory deadline of 1 month to reply to Subject Access Requests. The Council will use 30 calendar days to ensure compliance.

22. You should calculate the time limit from the day after the Council receives the request (whether or not this is a working day).

Note – The 30 calendar days begins as soon as a complete request is received anywhere within the Council. If a complete request is forwarded to you 10 days after it was received by a different team, you will only have 20 days to respond.

23. The timescale can be extended by a further 2 months in exceptional cases where requests are complex or where you have received a number of requests from an individual. Any extension to timescale should be agreed with the IMT Team and the individual must be informed within one month of the receipt of the request with an explanation as to why the extension is necessary.

24. Services need to provide information to IMT 10 days before the deadline to enable the response to be prepared.

Is the request correctly authorised?

25. If there are any doubts about the identity of the person making the request a signature and ID can be requested together with proof of address (e.g. a utility bill dated within the last 3 months.

26. A Subject Access Request can be made on behalf of someone. A third party can act on behalf of the data subject. We must receive written authorisation from the data subject that the third party is authorised to act on their behalf.

27. If a person lacks capacity to manage their legal, financial and health affairs. The Mental Capacity Act 2005 made provision for people to choose someone to manage not only their finances and property as well as make health and welfare decisions on their behalf. The authorisation is called a Lasting Power of Attorney (LPA). LPA's replaced Enduring Power of Attorney (EPA's) in 2007, when the Mental Capacity Act came into force. If someone lacks capacity, then a copy of the Lasting Power of Attorney must be seen before any information is released.

28. If there is Social Worker involvement with the applicant, please consult with the appropriate Senior Manager about the request as an application to the Court of Protection or other claim on the data subject's status as a competent individual might exist. If the third party is acting on behalf of the data subject, it must be based on written authorisation that satisfies the data controller. If further guidance is required, advice should be sought from Legal Services on the legal status of such authorisation.

29. Please note that the Data Protection Act covers any living individual, which means this right begins at birth. In most cases a parent can be considered as acting in the child's best interests. However, there may be a rare instance where this is not the case. If there is any doubt about whether the parent is acting in the best interest of the child by making the request, please consult a relevant Senior Manager or contact the Information Management Team.

30. Where the request is for a child's data, the maturity of the child to understand both the request and the consequences of disclosure must be considered. If there has been social work involvement, the Social Worker for the child should consider if the child is mature enough to understand the process and the consequences from disclosure.

31. The DPA2018 considers the age at which maturity to understand on line processing is age 13 and this should be considered as sufficient age and maturity to be able to exercise the rights of access. Please note that this is only a guide, as all children vary in their maturity and is not a legally binding age in England. We need to follow the ICO guidance and apply appropriate test outlined in that guidance before processing the request.
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Worked examples:

Situation 1: A solicitor requests all care records held for their client. They have written authorisation, signed by their client, stating the solicitors have the power to request anything on their behalf.

Release? **YES**. With signed authorisation a solicitor should be treated as if it was the applicant themselves applying. All personal information requested should be released.

Situation 2: A parent requests the records of their 10 year old child's involvement with Children's Services. They provide a copy of the birth certificate to prove they are the child's parent.

Release? **MAYBE.** Before the information is released the Social Worker responsible for the child's case should be consulted. A parent on a birth certificate may not have access or even contact with the child. Even if the parent is acting as the guardian of the child, the Social Worker should make a determination as to whether releasing the information is in the best interests of the child.

If the decision is made to release the information and the child is over 13, the Social Worker should contact the IMT to discuss if the child is mature enough to understand this request and the information that would subsequently be released. If so, the information may be released to the child and not the parent.

Situation 3: A claims handler for a car insurance company requests CCTV footage of a car accident involving one of their clients. They state that the policy gives them the right to act in the best interests of their clients.

Release? **NO**. Although the client may well have agreed to this verbally, they have not provided signed authorisation that the insurance company can access this data on their behalf. The insurance company may even be acting for a third party. They should be sent a copy of the SAR form and asked to both complete it and submit it, along with the written approval of their client, or to forward it to their client to submit directly.

Has the applicant provided specific scope for the request to enable us to find the information?

32. The applicant needs to provide enough information to allow us to find the requested information. As a large organisation, a request may cover a number of areas. It is reasonable for us to ask that an applicant to specify the information or processing activities to which the request relates. However, we **cannot** refuse a request if the applicant chooses not to do this.

33. If the applicant requests the release of "all the records" with no further direction then the Council is expected to perform a 'reasonable and proportionate' search. These requests should be forwarded to the Information Management Team (IMT) to coordinate. In the majority of cases, the service that the applicant writes to will be able to decide on what is reasonable as they are likely to be aware of the background to a request as it is unlikely to be beyond their service. If it is a multi-service request, then the IMT would co-ordinate the response.

34. If there is no local knowledge then a reasonable search of "all records" needs to be undertaken and the main systems would be searched and these would be:

- Council tax
- Housing benefit
- CRM system
- Social Care database
- Complaints

35. Where we process a large amount of information about an individual we can ask them for more information to clarify their request. If the request is manifestly unreasonable, the Council may charge a fee.

Note: When the Council requests a fee or further information to allow it to complete the request, the 1 month timeframe does not begin until this is received.

The applicant has 90 calendar days to provide this information. If the 90 days elapses without further contact from the applicant, the Council must write to them and confirm that the request has been closed.

Handling the request (Refer to Flow Chart A)

36. The Information Management Team (IMT) log, acknowledge and monitor Subject Access Requests. The request is forwarded to the relevant Service/ Team to provide the information. The Service/Team will have knowledge of the records and be able to alert the IMT if there are any issues or sensitivities with providing the information.

37. The Service/Team handling the request should provide all of the relevant information requested to the IMT. Any information that is withheld must be justified in writing.

38. The Service/Team handling the request also need to provide details of the privacy notice(s) that apply to the data to IMT so that information required in Article 15 can be provided to the applicant.

39. If the applicant is a Solicitor acting on behalf of a client, they may only receive the same information that would be released to the client, However care should be taken when releasing information to a third party. In the case of a solicitor, they will be acting under the direction of their client and in the client's best interest.

40. When a third party requests personal information the council must follow the instructions of the data subject as expressed in their letter of authorisation. If the request involves sensitive personal data or material the data subject may not know exists until that point, the council should, if possible discuss the consequences of disclosure with the data subject and their social worker, if they have one. However, under the Act there is no difference between a data subject and their agent, the authorised third party making a request on their behalf, in a subject access request.

What Information is an individual entitled to?

41. An individual is entitled to access any personal information that we hold on them either in electronic or paper format. For example, this would include case notes from SSID, Emails, Letters, Care Plans, Reports, and Contact Records. The list is not definitive or exhaustive. The guiding principle is that where the applicant's personal data is found, they have a right to access it unless an exemption applies.

42. As mentioned earlier, reasonable searches should be made on all major systems both electronic and manual to determine if personal information is held.

43. Access can be refused if a request has been made by a third party but the individual has made it clear that they do not want their personal information to be disclosed to that third party.

Exemptions to the right of access

44. There are several exemptions that apply to the right of subject access. The exemption means that the applicant is not entitled to receive the personal data.

45. A few that apply to the public sector are

a. Crime and Taxation (Information that would prevent the detection of crime or impede the collection of tax need not be released)

b. **Health, Social Work, and Education Data** - Information is withheld if it would, where the 'serious harm test' is met, be likely to prejudice the carrying out of social work, because it would be likely to cause serious harm to the physical or mental health of the data subject or another individual. The effect is to exempt personal data processed for these purposes from subject access to the extent that its disclosure would cause harm. This includes:
   - information which is processed by a court
   - consists of information supplied is evidence in the course of court proceedings
   - information given by the data subject which was provided in the expectation that it will not be disclosed,
   - access to child abuse data by an individual with parental responsibility where it would not be in the best interests of the child.

   These rules are set out in the DPA 2018 Schedule 3 :
   - Part 2- Health Data
   - Part 3 Social Work Data
   - Part 4 Education Data
   - Part 5 Child Abuse Data

c. **Judical Proceedings** – if information is shared it is likely to prejudice judicial proceedings (DPA2018 Schedule 11 Part 4(9)

d. **Confidential References** - If we send them, they are exempt, if we receive they are available. (DPA2018 Schedule 11 Part 4 (11))

e. **Management Forecasts or Planning** - If we are planning a restructure, the personal data is exempt to the extent that disclosure would undermine the forecasting or planning before the decisions are made. (DPA2018 Schedule 11 Part 4(8))

f. **Negotiations** - If we are negotiating with someone and the personal data would undermine that negotiation, it would be exempt until the negotiations end. (DPA2018 Schedule 11 Part 4(10))

g. **Legal Professional Privilege** (Information that is subject to legal professional privilege is exempt from disclosure unless the legal services waive that privilege. In all cases they must be consulted before using this exemption or disclosing material that has legal professional privilege. (DPA2018 Schedule 11 Part 4(9))

46. There may be other exemptions that apply so if you are concerned about the information that has been requested, please contact the Information Management Team.

47. Access can also be refused if a request has been made by a third party but the individual has made it clear that they do not want their personal information to be disclosed to that third party

48. Once you have gone through the various sources of personal information such as, files, folders, systems, you may find that you have personal information of other people in the same documents. Once you have identified the personal information of the applicant, the next step is to consider the personal information of other people. They are called the third party. The following describes what must be done with third party information.

Third Party Information

49. In a subject access request, the applicant is entitled to receive their personal data. The personal data of other people should only be disclosed as it relates by necessity to the request. For example, if an adult daughter attended a meeting with her mother, we would of necessity include the mother's name. By contrast, if the council had a meeting with the mother to discuss the daughter, their information also contains the mother's personal data. We would only disclose that information if other conditions were met. When we do have to withhold information, it should redacted (blacked out) so that the applicant can understand what was removed and why.

Please Refer to Third Party Flow Chart B

Steps to follow:

See if it is possible to remove the third party information from the page, leaving the applicants information intelligible. If so the applicant's information can be disclosed without the third party information.

- Signatures should **always** be redacted to guard against identity fraud
- Although the names of staff acting in a professional capacity would usually be left in, any personal contact details – home phone number or address – should be redacted
- Records of legal advice provided should not be released without the agreement of Legal and Democratic Services
- If a third party discussion is predominantly about the applicant, this can become their personal information even if they were not involved in the discussion

50. For more detailed guidance on redactions see Appendix 2. Advice and guidance on redactions can be also be sought from the IMT. When redactions are made, a copy of the redacted document and the original document must be sent to the IMT to ensure consistency.

51. The DPA2018 Schedule 2 Part 3 (16) states that where the data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information he is not obliged to comply unless

(a) The other individual has consented to the disclosure of the information to the person making the request, or
(b) It is reasonable in all circumstances to comply with the request without the consent of the other individual, (e.g. if the social work test or education test is met under Schedule 2 Part 3 (17)

52. In most cases, the council will rely on section (b). In those instances, the council has to consider whether it is reasonable in all circumstances that the information is to be released. In the Act, there is a test for reasonableness. The following statutory factors must be considered.

- Any duty of confidence owed to the third party
- Any steps taken by the data controller with a view to seeking the consent of the third party;
- Whether the third party is capable of giving consent; and
- Any express refusal of consent by the third party.

53. The third party in question should be informed, where possible, that disclosure is being considered. They may give consent to the information being released or raise any objections. However, even if objections are raised, the information should still be considered for release.

54. Please note that the council is not required to contact the third party. In some circumstances, this might not be possible, we do not know where the third party is located. However, if you decide not to contact the third party then that decision needs to be justified. When the council decides to disclose without contacting the third party, it will need to consider the possible effect of disclosure or the failure to disclose the personal information.

- The nature of the data and whether it might be damaging if disclosure or cause harm or bad feeling between the parties
- Whether approaching a third party may constitute a data breach e.g. the requester may not want the third part to know they have made the request (e.g. a family member)
- The nature of the third part's role are they acting in a formal role or official capacity or in a private and personal capacity
- Is the data already known to the data subject or something they would know by themselves
- Does the information have a particular importance to the applicant such as a claim or interest that needs to be weighed against the competing interest of the third party?

55. In many cases, the third party will include other professionals such as police, medical or other council officers. In these cases, disclosure is likely because they are acting in a professional or formal role. There may be cases where exemptions apply e.g. to Health or Social Care data where it may cause harm. The role of exemptions is discussed later.

56. After considering the statutory factors, and the nature of the data and its possible effects, the council is in position to decide whether the disclosure would be reasonable in all circumstances.

Worked example:

A member of staff requests copies of an interview conducted as part of a disciplinary case against them. Although the interview was between an investigating officer and a colleague of the applicant, the interview was wholly about the applicant.

This would most likely be seen to constitute the personal information of the applicant despite them not being involved in its creation. Steps should be taken to inform the investigating officer and colleague that this will be considered for release. As the personal data relates to their professional role, then it could be reasonable to disclose in all circumstances. However, if the employee has been threatened or is aware that disclosure will lead to recriminations, then those factors need to be considered before it can be considered reasonable to disclose.

57. Sometimes a request can lead to a large amount of documents being found and they need to be provided. Many people assume that the Act, is similar to FOIA where there is a fees limit that would avoid these requests. Unlike FOIA there is no fees limit in the DPA. However, if the search and the location of the personal data would constitute a **disproportionate effort**, then a request could be refused. Before deciding that a request is to be refused because of disproportionate effort to locate the information, consider whether you need to ask the applicant for more information to locate the information. If they can't or won't please contact the Information Management Team before refusing.

58. The Act covers personal information and is not a request for documents. However, a document can be considered a person's personal data. The ICO have instructed the council in the past to consider the document as person data. Please do not assume that a document is not to be provided. Where possible, a subject access request is to be answered with copies of the documents. If this cannot be met or there is a problem with supplying information in this way, then please consult with the Information Management Team.

59. No request should be refused without first seeking advice from The Information Management Team (IMT).

60. If a request cannot be completed within the 1month guideline, the applicant should be contacted to inform them of this. Where possible, reasons for the delay should be explained to the applicant, by an apology letter or email.

Completing the request

61. Once the information has been collated, a Senior Manager from the Service/Team should approve its release.

62. The standard response must include the following information:

a) The purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

63. If any information has been redacted, this should be stated in the response letter. Also it is considered good practice to explain why the material has been redacted. If an exemption is used, the exemption should be cited and explained. However we must avoid inadvertently revealing any information by explaining what has been removed.

64. A copy of the redacted information should also be kept by the service to ensure they are consistent if further information is requested.

65. Where the rights of the data subject are restricted, e.g. part or all of the information had been withheld, the data subject must be informed without undue delay:

(a) that the rights of the data subject have been restricted,

(b) of the reasons for the restriction,

(c) of the data subject's right to make a request to the Commissioner under

DPA2018 section 51(2), in order to check whether any restrictions imposed by the controller were lawful

(d) of the data subject's right to lodge a complaint with the Commissioner, and

(e) of the data subject's right to apply to a court under section 167 (Remedies in the Court) .

66. Where the information has been requested electronically (though the portal or by email), the information should be returned the same way in a commonly accessible format unless the requester has requested a specific format.

67. Where the information relates to a child who was previously looked after or an open case to social care, the information may be shared face to face by an experienced social care practitioner.

Correcting Information Held

68. Sometimes, following a SAR, an applicant notices that information held by the council may be inaccurate or out of date. They have a legal right to seek correction of the incorrect data.

69. To act in accordance with the Data Protection Act, the Council has a legal obligation to ensure that all information held is accurate. If, following the release of personal information, the applicant contacts the Council to highlight an error; this should be acknowledged and corrected as soon as possible. For example, a note can be placed in the file to explain what is considered wrong and the correct information noted. In some instances information cannot be deleted because it is still part of a record, so a note will be inserted with the correct information.

70. Requests to correct data can be made verbally or in writing and should be directed to the DPO@durham.gov.uk. Please see the information rights page for further information.

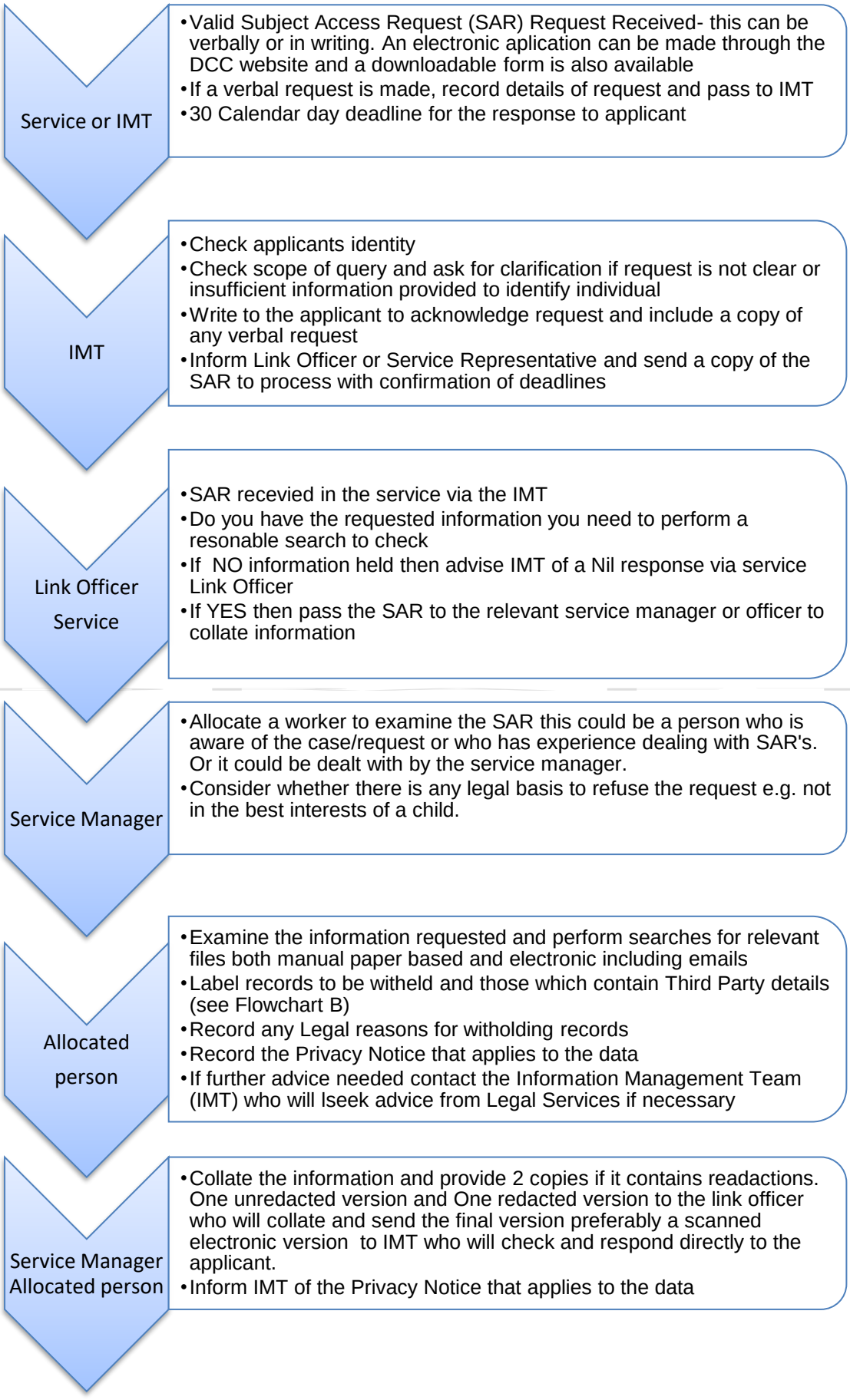
The ICO Subject access code of practice is contained in the link below. It provides further helpful guidance and information on the SAR process:

http://ico.org.uk/for_organisations/data_protection/subject_access_requests

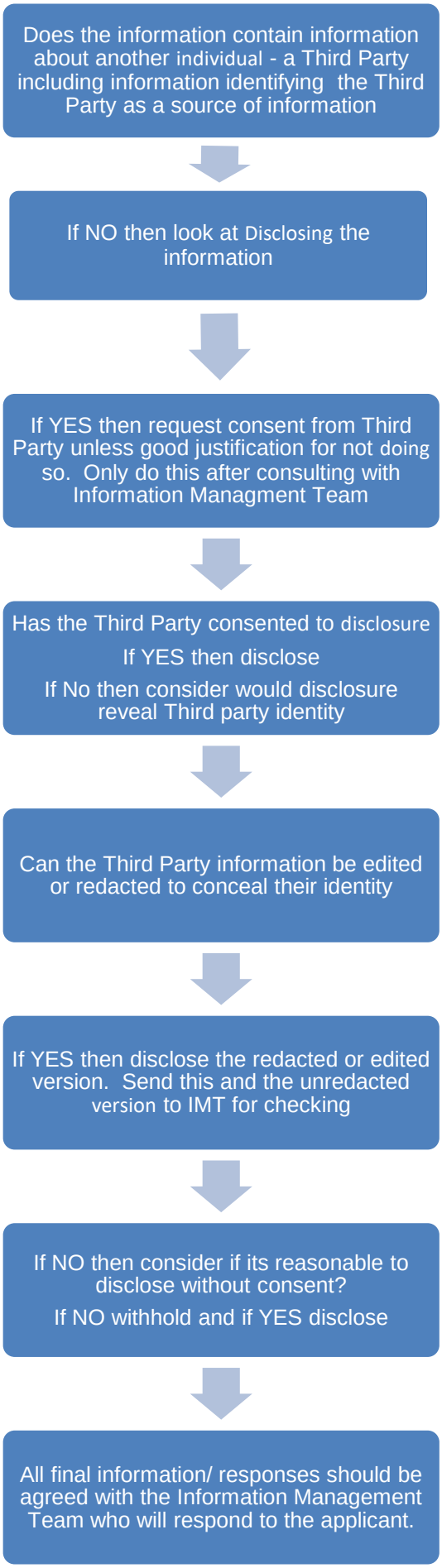
Useful Contacts

Information Management Team	dataprotection@durham.gov.uk 03000 268034
Lawrence Serewicz	Principal Information Management Officer Transformation and Partnerships 03000 268038 lawrence.serewicz@durham.gov.uk
Helen Lynch	Head of Legal and Democratic Services 03000 269729 Helen.lynch@durham.gov.uk
Keith Forster	Caldicott Guardian Strategic Manager, Operational Support CYPS 03000 267396 Keith.forster@durham.gov.uk
Data Protection Officer	Roger Goodes DPO@durham.gov.uk 03000 268050

Data Protection Act 2018 Subject Access Request Handling Flowchart A



Disclosure of Third Party Data Decision Flowchart B



List of Appendices

Flow Chart A – Subject Access Request Handling

Flow Chart B – Third Party Data Decision

Appendix 1 – Subject Access Request form

Appendix 2 – Redaction Guidance

Alternative formats