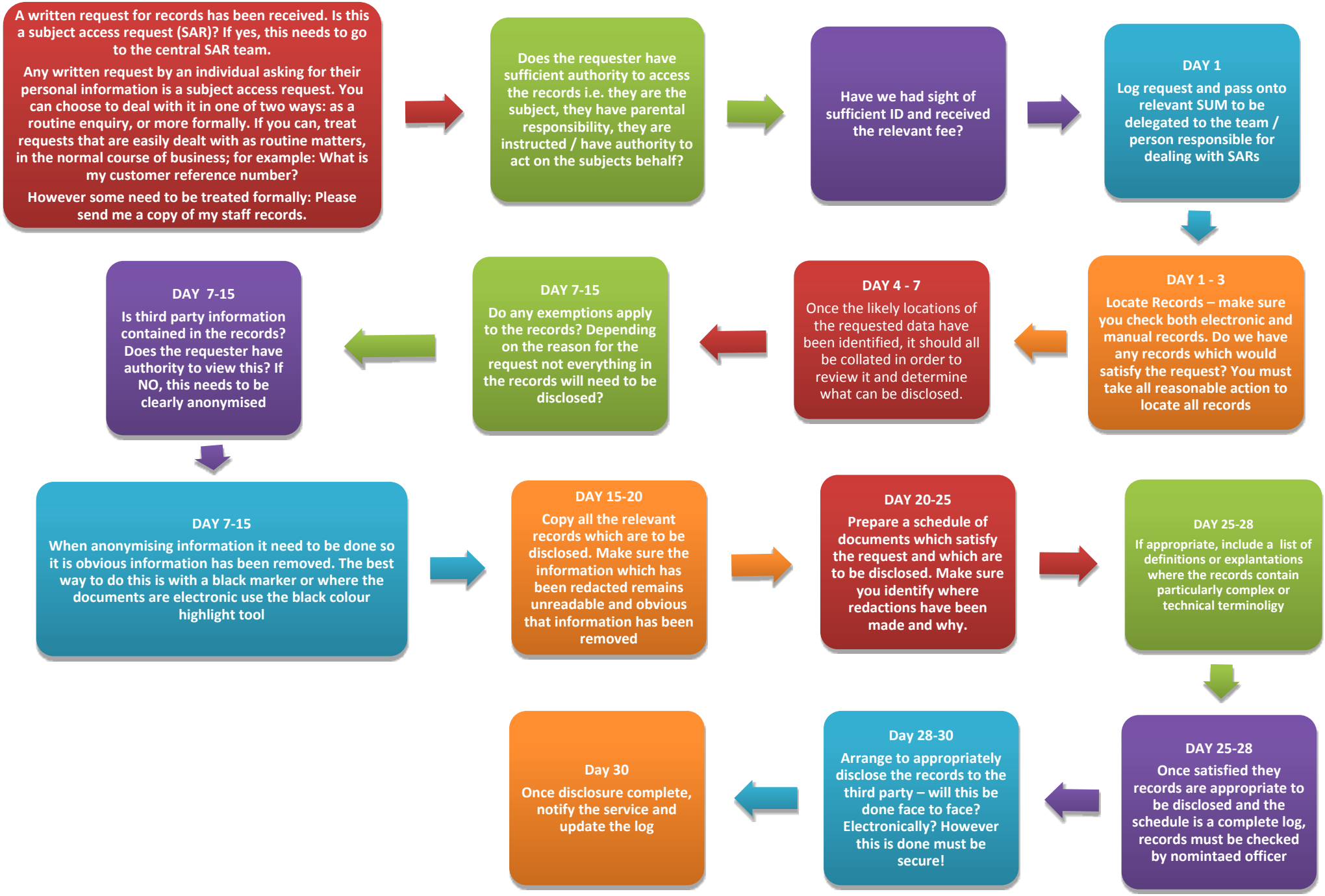
APPENDIX 12

Subject Access Request Guidance

May 2018

CONTENTS

1. SAR PROCESS FLOWCHART



2. INTRODUCTION

2.1 The Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) gives individuals the right of access to personal information held about them by an organisation. This right is set out in Article 15 of the EU General Data Protection Regulations (GDPR) and such a request is known as a 'subject access request' (SAR). The rights of subject access constitute a statutory duty and must be treated as a priority.

2.2 Failure to respond to a SAR within the legal timeframe may result in enforcement action brought by the Information Commissioner's Office (ICO) which is responsible for enforcing the DPA. It is imperative that all SARs are dealt with promptly. If you are unclear about your obligations, please seek advice as soon as possible. Details of who to contact for advice and assistance can be found at Part 10 of this Guidance.

3. SCOPE OF THIS GUIDANCE

3.1 This guidance has been drawn up to assist employees in understanding how to recognise and respond to a SAR in compliance with the Council's obligations under the DPA. It explains the right of access to personal data and the procedures that must be followed. A failure to follow this guidance may result in **disciplinary action**.

3.2 This guidance applies to all employees, including those who may respond to a SAR. It also applies to all personal information whether manual, electronic, audio or visual. This guidance should be read in conjunction with the Council's other related documents which include:

- Information Governance Framework – Conduct Policy
- Subject Access Requests - A basic guide to Redaction
- Pro-forma letters

These documents and other useful information can be found on the Council's Information Governance Intranet page.

4. THE RIGHT OF SUBJECT ACCESS

4.1 Individuals data rights are set out in the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) Almost all of these rights are subject to limitations and exceptions. The main right is that of subject access but there are others. The right of subject access includes access to *personal data*:

- processed electronically on a computer;
- Accessible records (for example housing tenancy files, social work files);
- Manual records held in a *relevant filing system;*
- In respect of public authorities subject to the Freedom of Information Act 2000 (FOIA) only, access to *unstructured* manual records which are not held in a *relevant filing system*.

4.2 The right of subject access allows a living individual ("the data subject") to find out what information ("personal data") is held by an organisation about them. Upon receipt of a valid SAR, the Council is required to provide the following information to the requester:

- Confirmation as to whether any personal data is being processed;
- A description of the personal data, the reasons it is being processed and whether it has/will be given to other organisations/people;
- A copy of the personal data (which may be copies of the original documents or a transcript which is specially prepared in order to respond to the SAR); and
- Details as to the source of the data (where this is available).

4.3 Information must be provided in a permanent format (e.g. by supplying copies of records where appropriate) and all information must be legible. Any acronyms or jargon should be explained to the data subject in the response. If a data subject only requires a copy of their personal data then you are not required to provide the other information listed above under (a), (b) and (d).

4.4 Further guidance on identifying personal information can be found at **Appendix 1**.

4.5 Under the General Data Protection Regulations the rights for individuals have been enhanced and further guidance is available on the Information Commissioner's Office website https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights. The following rights are now provided:-

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

5. ROLES AND RESPONSIBILITIES

5.1 Most SAR requests are sent directly to **Executive Support**, who will log the request and assign it to the appropriate officer within the relevant Directorate to deal with. Where a request is received by a service area directly, they will be responsible for ensuring that the request is logged within 24 hours of receiving it by sending a copy of the request by email to **Executive Support** (executivesuport@tameside.gov.uk)

5.2 All officers are responsible for recognising a SAR and following the appropriate steps to progress it, whether this means gathering the information requested personally, or transferring it to the appropriate person to deal with.

5.3 All managers/team leaders are responsible for being aware of the SAR procedure and cascading it to their team members. They are also responsible (where nominated by the Head of Service) for approving the response, notifying the **Directorate IG Champions** with issues and seeking advice and assistance where needed.

5.4 **Heads of Service**
Heads of Service are assigned responsibility for the main systems and information assets within their business area. The Head of Service is responsible for monitoring compliance with the DPA in respect of the information they 'own', which includes compliance with the right of subject access. They are responsible for selecting appropriate officers within their Service to be responsible for dealing with SARs and identifying different senior officers within their Service to act as Directorate IG Champions. In the event of a complaint about the way a SAR has been handled, the Head of Service is responsible ensuring the complaint is properly investigated and approving the response.

5.5 **Directorate IG Champions**
Directorate IG Champions have been appointed within Directorates to provide advice and support for officers who have been assigned a SAR to respond to. The Directorate IG Champions will also review information prior to disclosure following a SAR to ensure that the correct information is being disclosed and/or all appropriate redactions have been made.

In most cases an IG Champion will be a Service Unit Managers as they have an understanding of the service area and the information governance issues involved. They are also normally responsible for data protection or freedom of information as part of their job role.

All Directorate IG Champions will receive training in the handling of SARs and will therefore have a greater level of expertise than most officers in handling a SAR.

5.6 **Further Advice and Assistance**

There will be occasions where further advice and assistance is required.

- Process queries, should be directed to Executive Support (0161 342 3017)
- Disclosure/redaction queries should be directed in the first instance to the Risk and Insurance Team (0161 342 3859).
- Information Champions

6. WHAT MAKES A VALID SAR REQUEST?

6.1 **Time limit for complying with a SAR**

All SARs should be responded to promptly, and in most cases the maximum time limit for responding to a SAR is 1 calendar month once the following has been received by the Council:

- The written request;
- Clarification from the requester (where requested);
- Satisfactory proof of identity (where requested); and

6.2 **Request to be in writing**

A valid SAR must be made in writing, but it does not need to refer to legislation or mention the phrase "subject access". Even if the request refers to other legislation, such as the Freedom of Information Act, if it is a request for personal information of the person making the request (the data subject) it should be treated as a SAR. If the request refers to the Freedom of Information Act you will need to send a refusal notice relying on s40 (1) of the FOIA – see the attached link: - http://intranet2.tameside.gov.uk/corpserv/solicitor/proformadocs.doc .

6.3 Any written request which makes clear that personal information is being requested should be handled as a SAR and logged in accordance with the process set out in section four above.

6.4 The Council has a duty to make reasonable adjustments in the case of individuals who are disabled, so it may be appropriate as a reasonable adjustment to act upon a verbal request for information and handle it as a SAR. In such a case, the oral request should be documented in an accessible format and provided to the applicant or their advocate (if authorised) in writing so that both parties are clear about how the request is being handled.

6.5 In some cases, a request for personal data may be handled in the normal course of business, for example, if a customer asks for a further copy of information that they have misplaced. Such a request does not have to be dealt with formally as a SAR so long as it is dealt with promptly, and in any event, **within 1 calendar month**.

6.6 Some SARs may reach the Council through a third party that is processing personal data on the Council's behalf ("a data processor"). All SARs notified to the Council by a data processor must be dealt with as set out in this Guidance. In addition, receipt of a SAR from a data processor must be acknowledged in writing and clear instructions given as to any further information or action required from the data processor in dealing with the SAR.

6.7 **Asking for clarification**

If the wording of the request does not clearly identify the information that the requester is seeking, a letter must be sent to them promptly (and in any event within 3 working days) which asks them to provide further clarification to assist in locating the required information.

This might include asking the requester to identify particular departments, names of officers or specific dates etc., in relation to the information that they require. Whilst clarification can be sought, the requester must not be asked to narrow the scope of their request. If a requester has asked for "all information you hold about me", they are entitled to do so.

6.8 **Proof of identity**

It is important that the identity of the requester is verified to avoid information about one individual being sent to somebody else, either in error or as a result of deception. If the requestor is unknown to the employee processing the request, a letter must be sent to the requestor promptly (and in any event within 3 working days) asking them to provide two forms of identification, one of which should include their current address. If, following the provision of these documents, the employee processing the SAR is not satisfied about the identity of the requestor, they should contact the Directorate IG Champion.

Part 6 of this guidance explains what to do if a SAR is made by a third party on behalf of another person

6.10 **Requests made on behalf of others**

The DPA does not prevent an individual from giving permission to a third party to make a SAR on their behalf. For example, a data subject may instruct a solicitor, friend or family member to make a SAR on their behalf. It is up to the third party to provide satisfactory proof that they have been given authority to make the request. Documentary proof of this, such as a letter of authority signed by the data subject or a power of attorney, must be provided by the requestor. If there is any doubt about the authority given to the third party, information must not be disclosed and advice should be sought from the Directorate IG Champion.

7. REQUESTS FOR INFORMATION ABOUT CHILDREN

7.1 It is important to remember that personal data about a child, however young, is the child's personal data and is not the personal data of their parent or guardian. The age of consent for children is 13 as prescribed by Article 8 of the EU General Data Protection Regulations (GDPR).

7.2 A parent or guardian does not have an automatic right to personal data about their child and can only apply on the child's behalf if the child:

- has given consent; or
- is too young to have an understanding to make the application.

7.3 There is no fixed age at which a child may exercise their rights under the DPA, including the right of subject access. Any age may be appropriate if the young person has sufficient maturity/capacity. Children can make a subject access request if they are capable of understanding the nature of the request.

8. HANDLING THE SAR

8.1 Once a complete SAR is received, the 1 calendar month in which the SAR must be completed will commence. In the interest of good customer service, where possible we should aim to provide the requested information as soon as is practical. A **SAR Checklist**

should be completed at all stages. The flowchart at the beginning of this document gives guidance on the handling of a SAR.

8.2 In order for the Council to meet the statutory timescale the following timescales should be followed:-

- **Locating the requested information – Days 1-3**
  The location of all recorded data on the data subject, whether it is electronic or stored in paper files, must be identified within 3 days of receipt of the complete SAR. In many cases this will involve searching any electronic system used within your business area (e.g. ICS / IAS) and may also include a search of emails.

  Where it is identified that information is likely to be stored in email accounts, appropriate approval must be sought the process outlined in the ICT Security Access Procedure must be followed. A reasonable effort must be made to identify if any relevant information may be held within other service areas which should be disclosed as part of the SAR.

- **Collating the requested information - Days 4-7**
  Once the likely locations of the requested data have been identified, it should all be collated in order to review it and determine what can be disclosed.

- **Reviewing the information, deciding what to disclose, making the redactions and drafting the response letter – Days 7-15**
  The information must be carefully reviewed to determine whether some of it may be exempt from disclosure**. Further advice about whether an exemption applies may be required, so it is important that this process begins as soon as possible**. Further assistance is available in the guidance document "Subject Access Requests - A basic guide to Redaction"

  If there is information to be redacted (this means the removal of information from a document that should not be disclosed to the requester) the following process should be used:-
  - Information to be redacted should be approved be the Directorate IG Champion before the source material is copied.
  - Once approved, the source material should be copied on single sided A4 paper and any redactions carried out manually using a black marker or electronically using Adobe Acrobat or bespoke redaction software.
  - The Quality Assurance step detailed below must be followed before any information is disclosed to the requestor.

  If information is withheld in reliance on an exemption, the requestor is entitled to receive an explanation in plain English detailing the fact that information has been withheld and the reasons why. The explanation must be more than simply specify that a particular exemption applies.

- **Quality Assurance – Days 25-28**
  In any case where it is proposed that an exemption should apply in order to withhold or redact information, this must be reviewed by an appropriate other person. This will normally be the Directorate IG Champion. The proposed response letter and information should be referred to the Directorate IG Champion together with the IG Checklist.

  The Directorate IG Champion will then be required to review the proposed response and information to check that the use of exemptions is appropriate. The Directorate IG Champion must complete the Quality Assurance section of the SAR Checklist.

This should then be referred back to the officer handling the SAR, who will be responsible for making the final disclosure.

- **Making the disclosure – Days 28-30**
  Every effort should be made to ensure that the response letter is addressed to the correct person, has the correct address and the information being disclosed is about the right person. The response must be sent by a suitably secure method, and evidence of this must be retained. For example, if being sent by post, the response should be sent by Royal Mail Signed for Delivery, and where the response is sent by email, the content should sent using Egress Switch.

  All documents disclosed to the requester must be listed on a document schedule **(Appendix 2)** which will include details of the justification behind information being redacted. Copies of the documents that have been disclosed to the requester must be marked with **"Redacted documents disclosed to the Data Subject"** and retained. A complete copy of the un-redacted documents must also be retained.

- **Delays**
  If there will be a delay in providing a complete response to the SAR, for example because of the volume of information or the complexity in redacting the information, the officer handing the SAR must notify **Executive Support who can then inform the requestor**. As much information as possible should be given within the 40 day time limit and only delay responding where this is unavoidable. This is important to ensure good customer service and to provide as evidence to the Information Commissioner (where appropriate) in respect of a complaint about any delay in responding to a SAR.

  Failure to comply with the 40 days allowed to respond to a SAR may leave the Council open to not only reputational damage and the scrutiny of the Information Commissioner but also potential enforcement action and fines. Where staff fail to comply with this statutory duty under the Data Protection Act disciplinary action may be taken.

8.3 **Format of information**
In order to comply with a SAR, in many cases it will be convenient to supply the requester with copies of documents (redacted where appropriate). However, the right of subject access under the DPA is not a right to copies of documents. In some cases, SAR compliance may be achieved by producing a transcript of the personal data and supplying this to the requester, rather than providing heavily redacted documents. Must be in a clear, easily accessible format, where possible electronic

9. REQUESTS INVOLVING THIRD PARTY PERSONAL DATA

9.1 The Council does not have to comply with a SAR to the extent that it would mean disclosing information about another individual who can be identified from that information, except where either:

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

9.2 In many cases the requested information will include the personal data of the requester and will also identify other people. Where information relates to the data subject and also includes information about another individual, an assessment will need to be made as to whether information identifying another person should be disclosed. For the avoidance of

doubt, information that solely relates to the data subject who has submitted the SAR must be disclosed (unless it is otherwise exempt).

9.3 The ICO has issued a **Subject Access Code of Practice** which provides guidance on the handling of SARs. It suggests three steps when handling SARs involving other people's information. These are summarised below.

- **Step One: Does the request require the disclosure of information that identifies a third party?**
  The ICO suggest that when considering whether it is possible to comply with the request without providing information that identifies other individuals, you should take into account any information that you disclose and also any information you reasonably believe that the requester may have, or may get hold of, that would identify the third party(ies).

  If it is possible to do so, then names/information about third parties can be redacted or withheld when making the disclosure. If it is not possible to separate the third-party information from the personal data of the data subject making the SAR, then Steps Two and Three should be considered.

- **Step Two: Has the third-party individual consented?**
  If it is appropriate to seek consent, and the third party does consent, the information can be disclosed. There is no obligation under the DPA to seek consent, and sometimes this will not be possible, for example in relation to old social work records when the whereabouts of individuals will be unknown.

  In some cases it may not be appropriate to seek the consent of the third party; for example, where the third party is a perpetrator/alleged perpetrator of abuse against the data subject, it may be ill-advised to approach the third party especially as this will inevitably involve a disclosure to them about the SAR that has been made. If it is not appropriate or possible to seek consent, or where consent has been refused, then Step Three should be considered.

- **Step Three: Would it be reasonable in all the circumstances to disclose without consent?**
  An assessment as to whether it would be reasonable in all the circumstances to make the disclosure will need to be undertaken. This assessment would be best undertaken by, or in consultation with, an officer who has been involved in dealing with the data subject or is at least aware of the circumstances of the case. In cases where the information is not recent, it is accepted that this will not be possible and therefore the assessment of what it reasonable will need to be undertaken by an officer having read the paperwork.

9.4 The DPA itself suggests various factors which ought to be considered when deciding whether it is reasonable to disclose information where a third party would be identified. These factors are:

- Any duty of confidentiality owed to the third party;
- Any steps taken to try to obtain the consent of the third party;
- Whether the third party is capable of giving consent;
- Express refusal of consent of the third party.

9.5 **Duty of confidence owed to a third party**
A duty of confidence can arise where information has the necessary quality of confidence (which means that it is not generally available to the public and is not trivial) and is imparted in circumstances whereby the party making the disclosure has a reasonable expectation that the information will remain confidential. Some relationships carry a general duty of

confidence e.g. doctor/patient, solicitor/client. As a general rule, where a duty of confidence is owed to a third party, it would not be reasonable to disclose such information. Advice should be sought if the employee dealing with the SAR is unsure.

9.6 **Other relevant factors**

The ICO's guidance also suggests other relevant factors that may be considered: "Information generally known by the individual making the request. If the third party information has previously been provided to the individual making the request, is already known to them, or is generally available to the public, it will be more likely to be reasonable for you to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual."

9.7 **Circumstances relating to the individual making the request**

The importance of the information to the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life. Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent."

9.8 **Information about Council officers**

As a general presumption, information identifying Council officers acting in their professional capacity may be disclosed. However, this should be considered on a case by case basis according to the principles outlined above. Advice should be sought if the employee dealing with the SAR is unsure.

There are special rules about the disclosure of third party data where the third parties are professionals in health, education or social work. In general terms, such information does not need to be redacted unless disclosure of the officer's identity would put their health and safety at risk. Advice should be sought if the employee dealing with the SAR is unsure.

10. EXEMPTIONS

10.1 In some cases exemptions may be applied, which means that certain information may not need to be disclosed to the data subject in response to their SAR. The DPA includes a number of exemptions but this Guidance only explains those which are most relevant to the information held by the Council. If there are still concerns about disclosing information, then advice should be sought from your Directorate IG Champion.

10.2 **Third Party Information**

As a general rule, information about third parties should not be disclosed without that person's consent. There will be times when it would not be possible or appropriate to seek consent of the third party, so you will then need to consider whether it is reasonable to disclose information that identifies a third party. For example, it may be reasonable to release names of third parties without seeking express consent, i.e. where it is clear that the enquirer already knows the information about the third party.

10.3 **Crime and taxation**

Information can be exempt if the disclosure of that information in response to the SAR would prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or the collection of any tax or duty. For example, this might apply to information about an individual that has been shared with the Police in respect of an ongoing investigation. It might also apply to information about an individual who is being investigated for council tax fraud.

If this exemption does apply to information, care must be taken when responding to the SAR. In some cases, the response may "tip off" an individual by explaining the reasons why information is being withheld under this exemption. It is therefore suggested that advice is sought where this exemption applies.

10.4 **Health, social work and education**

Some information relating to health, social work and education may be exempt from disclosure in certain circumstances. If the documents include medical information, which came from a health professional, the general rule is that a health professional must be consulted to establish whether disclosing the information could be detrimental to the individual concerned. There are exceptions to this so advice must be sought where there is doubt about whether consultation with a health professional is required.

If the documents include health data about the requester (other than information which was provided by a health professional) and it is considered that disclosure may cause serious harm to the physical or mental health of the individual or any other person, advice should be sought as there may be requirement to consult with a health professional before any disclosure is made.

Special rules apply where releasing information about social services and related activities that could impact on delivery of social work by causing serious harm to the physical or mental health of the individual or any other person. Any such information must be redacted. Occasions where this exemption applies are few but if it may apply, the relevant and involved Social Worker must be consulted and advice sought from the Directorate IG Champion. Data should not be withheld simply because the individual is likely to make a complaint about a social worker when they see the information.

10.5 **Confidential references**

A reference provided by the Council about the data subject to another party is exempt from disclosure. A reference received by the Council from another party will not be caught by this exemption.

10.6 **Publicly available information**

Any personal data that the Council is required to publish is exempt.

10.7 **Negotiations with the requester**

This exemption may apply to information about the Council's intentions in negotiations with an individual to the extent that complying with a SAR would be likely to prejudice the negotiations. For example, this exemption might apply in relation to negotiations relating to Employment Tribunal proceedings.

10.8 **Legal professional privilege**

Where legal advice has been sought or where there are or have been legal proceedings, information may be covered by legal professional privilege and may be exempt from disclosure. **Legal Services should always be consulted in these cases before making any disclosure**.

11. COMPLAINTS ABOUT SUBJECT ACCESS

11.1 Where a requester is not satisfied with the response to their SAR, the Council offers an internal review. Where a complaint is received, a senior manager (who will not be the officer who made the original decision) must immediately notify Sandra Stewart as the Data Protection Officer. The senior manager must then investigate the complaint and report to Sandra Stewart within 5 working days on the outcome of the investigation.

11.2 In addition to the internal review process, a data subject may also refer their complaint to the ICO, or may take action through the courts to enforce their right of subject access.

11.2 A separate protocol is in place for dealing with requests from the Police and the Crown Prosecution Services (CPS) and the Single Point of Contact (SPoC) is Danielle Cunningham-Hobbs (Risk, Insurance and Information Officer) within the Risk Management and Audit Service.

IDENTIFYING PERSONAL DATA **APPENDIX 1**

Q1 - Can a living person be identified from the information or in conjunction with that and other information held by the Council?	• Yes - Proceed to Q2 • No - Not personal data • Unsure - Proceed to Q2
Q2 - Does the information relate to an individual (in a personal or professional sense)?	• Yes - It is likely to be personal data • No - Not personal data • Unsure - Proceed to Q3
Q3 - Is the information 'obviously about' a particular individual?	• Yes - It is personal data • No - Proceed to Q4 • Unsure - Proceed to Q4
Q4 - Is the information 'linked to' an individual so that it provides particular information about an individual?	• Yes - It is personal data • No - Proceed to Q5 • Unsure- Proceed to Q5
Q5 - Is the information used, or will it be used, to inform/influence actions or decisions affecting an identifiable person?	• Yes - It is personal data • No - Proceed to Q6 • Unsure - Proceed to Q6
Q6 - Does the information have any biographical significance to the individual?	• Yes - It is likely to be personal data • No - Proceed to Q7 • Unsure - Proceed to Q7
Q7 - Does the information focus/concentrate on the individual as its central theme, rather than another individual, object, transaction or event?	• Yes - It is likely to be personal data • No - Proceed to Q8 • Unsure - Proceed to Q8
Q8 - Does the information impact or have the potential to impact on the individual, in personal, family, business or professional capacity?	• Yes - It is likely to be personal data • No • Unsure - Seek advice from Legal Services or Risk Management

SCHEDULE OF DISCLOSED DOCUMENTS **APPENDIX 2**

SCHEDULE OF DOCUMENTS DISCLOSED IN RESPONSE TO SUBJECT ACCESS REQUEST		
Ref	**Page No.**	**Details (including redaction rationale)**
1	If only providing part of a report list which page number i.e. 8-10	Example….Psychological report of parent dated 01/01/2010 As the information relates mainly to the parent and their relationships/health etc. the report has been redacted to protect the third parties information as this is either unknown to the requester or protected information.
2		
3		
4		