APPENDIX 1

Subject Access Request Guidance

Date: December 2021

Version: V2.0

APPENDIX 1

Document Version Control

Document Version Control		
Version	**Date**	**Approved by**
1.0	May 2018	Audit Panel – 29 May 2018
2.0	December 2021	Information Governance Group – 2 December 2021
2.0	March 2022	Audit Panel – 15 March 2022

This is a live document effective from the issue date. It supersedes any previous versions of this document, which are now withdrawn.

APPENDIX 1

Contents

SAR PROCESS FLOWCHART 4
1. INTRODUCTION 5
2. DEFINITIONS 5
3. SCOPE OF THIS GUIDANCE 6
4. THE RIGHT OF SUBJECT ACCESS 7
5. ROLES AND RESPONSIBILITIES 7
5.2. Employees 7
5.3. Managers 7
5.4. Heads of Service 8
5.5. Directorate IG Champions 8
5.6. Subject Access Request Coordinator (Children's and Adult's Services) 8
6. WHAT MAKES A VALID SAR REQUEST? 8
6.1. Format of request 8
6.2. Asking for clarification 8
6.3. Proof of identity 9
6.4. Requests made on behalf of others 9
7. REQUESTS FOR INFORMATION ABOUT CHILDREN 9
8. HANDLING THE SAR 9
8.1. Time limit for complying with a SAR 9
8.2. Process for handling a SAR 10
8.3. Format of information being disclosed 12
9. REQUESTS INVOLVING THIRD PARTY PERSONAL DATA 12
9.4. Duty of confidence owed to a third party 13
9.5. Other relevant factors 13
9.6. Information about Council officers 13
10. EXEMPTIONS 14
10.2. Crime and taxation 14
10.3. Health, social work and education 14
10.4. Confidential references 14
10.5. Publicly available information 15
10.6. Negotiations with the requester 15
10.7. Legal professional privilege 15
11. COMPLAINTS ABOUT SUBJECT ACCESS 15
APPENDIX 1 16
REDACTION GUIDANCE 16

SAR PROCESS FLOWCHART

APPENDIX 1

A written or oral request for records has been received.

Is it a SAR?

If yes, this needs to go be forwarded to the Information and Improvement Team to coordinate.

Does the requester have sufficient authority to access the records i.e. are they data subject, do they have power of attorney etc?

Have we had sight of sufficient evidence to confirm the identity of the requester/data subject?

Do we need to clarify the request? If so, send response to requester within 3 working days of the request and seek clarification.

The 1 month time limit pauses until clarification is received.

DAY 1

Log request and pass onto relevant SUM to be delegated to the team/person responsible for dealing with SARs.

Day 1 – 3

Locate records – make sure you check both electronic and manual records. Do we have any records which would satisfy the request? You must take all reasonable action to locate all records.

Day 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 data can be disclosed.

Day 7 – 15

Do any exemptions apply to the records? Depending on the reason for the request not everything in the records will need to be disclosed.

Day 7 – 15

Is any third party information contained in the records? Does the requester have authority to view this? If NO, this needs to be clearly anonymised.

Day 7 – 15

Any information to be anonymised needs to be redacted with the approved redaction software. The use of black marker is strictly prohibited and all paper records must be scanned into electronic format for redaction.

Day 15 – 20

Copy all the relevant records which are to be disclosed. Make sure the information which has been redacted remains unreadable and obvious that information has been removed.

Day 20 – 25

Prepare a Schedule of documents which satisfy the request and which are to be disclosed. Make sure you identify where redactions have been made and why.

Day 7 – 15

If appropriate, include a list of definitions or explanations where records contain particularly complex or technical terminology.

Day 25 – 28

Once satisfied the records are appropriate to be disclosed and the schedule is a complete log, records must be checked by a nominated officer.

Day 28 – 30

Arrange to securely disclose the records, usually in the same format as the request (so electronic disclosure where the request was made electronically etc. unless the requester specifies otherwise).

Day 30

Once disclosure complete, notify the service and update the log.

APPENDIX 1

1. INTRODUCTION

1.1. The Data Protection Act 2018 ("DPA 2018") and General Data Protection Regulations ("UK 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 UK GDPR and s.45 DPA 2018 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. It is imperative that all SARs are dealt with promptly and within the statutory timescales.

1.2. Failure to respond to a SAR within the statutory timescales may result in enforcement action brought by the Information Commissioner's Office (ICO). If you are unclear about your obligations, please seek advice as soon as possible, from the following:

- For process queries, you should contact the Information and Improvement Team (informationandimprovement@tameside.gov.uk / 0161 342 3017)
- Disclosure/redaction queries should be directed in the first instance to the Information Governance Team (information.governance@tameside.gov.uk / 0161 342 2170).
- Information Champions.

2. DEFINITIONS

2.1. The following terms are used throughout this document and are defined as follows:

Table 1 – Definitions

Term	Definition
Personal Data	Is any personal data as defined by UK GDPR and the Data Protection Act 2018. It is defined in the Data Protection Act 2018 at **s.3(2)** as "any information relating to an identified or identifiable living individual." Broadly, this means any information (relating to a living individual who can be identified or identifiable, directly from the information in question, or indirectly identified from that information in combination with other information that is in the possession of the Council. The UK GDPR provides a non-exhaustive list of identifiers, including: • Name; • Identification number; • Location data; and • Online identifier (e.g. IP addresses). Personal data also applies to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living person. The Council is legally responsible for the storage, protection and use of personal data / information held by it as governed by UK GDPR and the Data Protection Act 2018.

Term	Definition
Special Category Data	This data is covered by Articles 6 and 9 of the General Data Protection Regulations (UK GDPR). As it is more sensitive it needs more protection and consists of: • Racial or ethnic origin • Political opinions / beliefs • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data (where used for ID purposes) • Health; • Sex life; or • Sexual orientation. Criminal Offence Data is not Special Category Data, but there are similar rules and safeguards for processing this type of data.
Protected Information	Is any information which is: Personal / Special Category Data; or Confidential to the Council and which could have adverse consequences for the Council if it was released in an uncontrolled way.
Employee(s)	Includes all employees, Members of the Council, Committees, temporary staff, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.
Redaction	Is a process that is undertaken to render data/information unreadable. This is done by blocking out individual words, sentences or paragraphs or by removing whole pages or sections prior to the release of the document. Redactions should not just be a blank space, it should be clear that redactions have been made to a document and the amount of information redacted should also be clear.

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 2018 and UK GDPR. It explains the right of access to personal data and the procedures that must be followed. 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 and should be read in conjunction with the Council's other related documents, found on the Council's Data Protection/Information Governance Intranet page.

4. THE RIGHT OF SUBJECT ACCESS

4.1. 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 2000") only, access to unstructured manual records that 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:

(a) Confirmation as to whether any personal data is being processed;
(b) A description of the personal data, the reasons it is being processed and whether it has/will be given to other organisations/people;
(c) 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
(d) 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**.

5. ROLES AND RESPONSIBILITIES

5.1. Most SAR requests are sent directly to the Information and Improvement Team (Executive Support), who log and acknowledge the request and will, if required, conduct identification checks and seek clarification of the SAR. They will then hand over the SAR to the appropriate officer within the relevant Directorate to review and respond. 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 Information and Improvement (informationandimprovement@tameside.gov.uk).

5.2. Employees

5.2.1. All employees 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. Managers

5.3.1. All managers are responsible for being aware of the SAR procedure and ensuring compliance by 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

5.4.1. 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 2018/UK GDPR in respect of the information they 'own', which includes compliance with the right of subject access. They are responsible for selecting appropriate employees within their Service to be responsible for dealing with SARs and identifying different senior employees 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 for ensuring the complaint is properly investigated and approving the response.

5.5. Directorate IG Champions

5.5.1. Directorate IG Champions have been appointed within Directorates to provide advice and support for officers in relation to data protection and information governance matters and can assist with SARs or signpost further support.

5.6. Subject Access Request Coordinator (Children's and Adult's Services)

5.6.1. Children's and Adult Services have their own SAR Request Coordinator, Danielle Cunningham-Hobbs (d.cunningham-hobbs@tameside.gov.uk). All SARs for Children's or Adults Services data should be referred to the Information and Improvement Team in the first instance, who will then liaise with the SAR Coordinator to fulfil the request. All employees within Children's and Adults Services are required to assist the SAR Coordinator where required.

6. WHAT MAKES A VALID SAR REQUEST?

6.1. Format of request

6.1.1. A valid SAR can be made either verbally or in writing, including on social media. The request does not need to refer to legislation or mention the phrase "subject access".

6.1.2. Even if the request refers to other legislation, such as the FOIA 2000, 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 to the FOI request relying on s.40(1) of the FOIA 2000, though the SAR will still have to be dealt with within the appropriate timescales.

6.1.3. 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.

6.1.4. 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.

6.2. Asking for clarification

6.2.1. If the wording of the request does not clearly identify the information that the requester is seeking, a response 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.

6.2.2. 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, it should only be used when clarification is genuinely needed and not as a stalling tactic. Additionally, 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.

6.3. Proof of identity

6.3.1. 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. Where necessary, the Information and Improvement Team will, as part of their initial response, ask the requester to provide two forms of identification, one of which should include their current address. The initial response and any ID requests that are required must be sent as soon as possible, and no later than 3 days after the SAR request is received, so it is important that any SAR requests received directly by service areas are forwarded to Information and Improvement Team as soon as possible.

6.4. Requests made on behalf of others

6.4.1. A SAR can be made directly by the data subject, or by a third party on their behalf (e.g. a Solicitor, relative or friend). Documentary proof of this, such as a Form of Authority signed by the data subject or a Power of Attorney, must be provided by the requester. 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 Information and Improvement Team.

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 UK 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 2018/UK GDPR, 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. Time limit for complying with a SAR

8.1.1. All SARs should be responded to promptly, and in most cases the maximum time limit for responding to a SAR is one calendar month from the date the request was received. This time limit can be paused where:

- Clarification of the request is sought from the requester;
- We request proof of identity from the requester.

8.1.2. The time limit pauses at the point our request is made and resumes again once the additional information is provided to us. Whenever requesting clarification of the request, you must inform the requester that the time limit has been paused in order to manage their expectations.

8.1.3. The time limit for responding to a SAR can also be extended by a further two months if the request is complex or we have received a number of requests from the individual relating to individuals' rights. Where the time limit is being extended, we must inform the requester at the earliest stage possible in order to manage their expectations.

8.1.4. 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. Process for handling a SAR

8.2.1. In order for the Council to meet the statutory timescale the following timescales should be followed:

8.2.2. Days 1–3 – Acknowledging the request/conducting ID checks/requesting clarification/locating the requested information

8.2.2.1. All Subject Access Requests should be forwarded to the Information and Improvement Team in order to manage the request. An acknowledgment will be sent to the requester and proof of ID will be requested. If necessary, clarification of the request will be sought as soon as possible, and within 3 working days at the maximum.

8.2.2.2. 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.

8.2.2.3. Where it is identified that information is likely to be stored in email accounts, the officer allocated the SAR must determine who may have emails related to the SAR and request them as a matter of urgency. 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.

8.2.3. Days 4-7 - Collating the requested information

8.2.3.1. 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.

8.2.4. Days 7-15 - Reviewing the information, deciding what to disclose, making the redactions and drafting the response letter

8.2.4.1. 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.

8.2.4.2. 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:

- Any queries with information to be redacted should be discussed with the Information and Improvement Team, SAR Coordinator, Information Governance Team, Legal Services or the Directorate IG Champion;

- Once approved, all records should be redacted electronically using the Council's approved software.
- All paper records should be scanned into the system in order to convert them so they can be redacted using the software.
- For the avoidance of doubt, the use of a black marker to redact paper records is strictly prohibited as it does not always fully obliterate the data underneath and can allow the requester to identify information they are not permitted to view. In a similar vein, the use non-authorised software or IT tools (such as highlighting over a word in black on Microsoft Word) are strictly prohibited, as the redactions can be completely undone with relative ease.
- Use of any method of redaction other than the approved software will be a breach of this guidance, may lead to the occurrence of a data breach and may lead to disciplinary action;
- The redacted document(s) should be reviewed by a second person to ensure that all data that requires redaction has been redacted and that the redaction cannot be undone;
- The Quality Assurance step detailed below must be followed before any information is disclosed to the requester.

8.2.4.3. If information is withheld in reliance on an exemption, the requester 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.

8.2.5. Days 25-28 - Quality Assurance

8.2.5.1. 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 a Manager but could be the Directorate IG Champion. The proposed response letter and information for disclosure should be referred back to management for review before it is sent to the data subject.

8.2.5.2. Best practice states that the manager should review the proposed response and information to check that the use of exemptions is appropriate and 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.

8.2.6. Days 28-30 - Making the disclosure

8.2.6.1. Every effort should be made to ensure that the response is addressed to the correct person, has the correct contact details (email/address as appropriate) and the information being disclosed is about the right person.

8.2.6.2. The format for the response to a SAR is usually dependant on how the request was made. Requests made electronically (via email or social media) will usually necessitate a response by electronic means, with the information in a commonly used electronic format, unless the requester has asked for a reasonable alternative means to be used. Disclosure should not be made through social media and instead sent via email. Any email disclosure should be sent securely using Egress. It is appropriate to respond by post in some circumstances (where request by post), although if email can be used it is the preferred option as it is more secure.

8.2.6.3. It is best practice in all cases to confirm how the requester wants to receive the disclosure and in what format it should be provided. Secure email is the default and preferred method of disclosure where the content of the disclosure is particularly sensitive (e.g. Children's Services records) and the requester should be directed towards using secure email where

possible even if they initially indicate a different method for the response. In the rare circumstance that the requester cannot accept disclosure by secure email, then it may be appropriate to provide the information in hard copy postal delivery. As a minimum standard, any postal delivery must be sent by Royal Mail Signed for Delivery and proof of postage and receipt should be retained on file. Confirmation of receipt should also be sought from the requester on conclusion of the case.

8.2.6.4. If the response in paper format is large or Royal Mail delivery is not considered to be appropriate, hand delivery/delivery by courier, or collection of the response by the data subject could be considered with appropriate ID in place.

8.2.6.5. All documents disclosed to the requester must be listed on a document schedule, 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.

8.2.7. Delays

8.2.7.1. 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 the Information and Improvement Team who can then inform the requester. As much information as possible should be given within the 1 calendar month 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 ICO (where appropriate) in respect of a complaint about any delay in responding to a SAR.

8.2.7.2. Failure to comply with the 1 calendar month allowed to respond to a SAR may leave the Council open to not only reputational damage and the scrutiny of the ICO but also potential enforcement action and fines. Where staff fail to comply with this statutory duty under the DPA 2018/UK GDPR disciplinary action may be taken.

8.3. Format of information being disclosed

8.3.1. 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 2018/UK GDPR 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.

8.3.2. All information disclosed, whether in the form of a redacted document or a transcript, must be in a clear, easily accessible format.

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 DPA 2018/UK GDPR 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.

9.4. Duty of confidence owed to a third party

9.4.1. 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.

9.4.2. 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.

9.4.3. Advice should be sought if you are unsure whether confidentiality applies to any information requested under a SAR.

9.5. Other relevant factors

The ICO's guidance also suggests other relevant factors that may be considered.

9.5.1. <u>Information generally known by the individual making the request.</u>

9.5.1.1. It is more likely to be reasonable for you to disclose the information if:

- The individual making the request has previously received the third party information;
- The requester already knows the information; or
- The information is generally available to the public.

9.5.2. <u>Circumstances relating to the individual making the request</u>

9.5.2.1. 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.

9.6. Information about Council officers

9.6.1. 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.

9.6.2. There are special rules about the disclosure of third party data where the third parties are professionals in health, education or social work, (see Section 10.3 below). 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 2018/UK GDPR includes a number of exemptions but this Guidance only explains those that 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. Crime and taxation

10.2.1. 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.

10.2.2. 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.

10.3. Health, social work and education

10.3.1. 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.

10.3.2. 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.

10.3.3. 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.

10.4. Confidential references

10.4.1. A reference provided in confidence about the data subject will be caught under this exemption. This applies whether the reference was given or received by the Council and applies to both companies involved. If the reference is not given or received in confidence, then the exemption will not apply.

10.5. Publicly available information

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

10.6. Negotiations with the requester

10.6.1. 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.

10.6.2. This exemption does not set out any limits regarding the timing of negotiations and does not require that negotiations still be ongoing. You may be able to apply the exemption after negotiations have ended, but only if you can justify why it would be likely to prejudice negotiations, i.e. it would prejudice the Council's position in future negotiations. The key is that we must be able to demonstrate that complying with the SAR will prejudice the Council's position.

10.7. Legal professional privilege

10.7.1. 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.

10.7.2. 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 directly by the service the Information and Improvement Team must be notified as a matter of urgency so that the appropriate course of action can be determined.

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.

11.3. A separate protocol is in place for dealing with requests from the Police and the Crown Prosecution Services (CPS). Requests of this nature in relation to Children are sent to the Single Point of Contact (SPoC), Danielle Cunningham-Hobbs (Children's Services). Other requests may be received by Exchequer Services or the Risk, Insurance and Information Team.

APPENDIX 1

REDACTION GUIDANCE

The below guidance is an extract from the Redaction Guidance Document which can be found on the Data Protection/Information Governance Framework. Employees are directed to review the full Redaction Guidance.

1. WHAT IS REDACTION?

1.1. Redaction is a process which is undertaken to render data/information unreadable. There may be different reasons why data/information should be withheld, but one common reason for redacting documents and files is to ensure information about others is not disclosed inappropriately when sending out responses to SARs.

1.2. Redaction is done by blocking out individual words, sentences or paragraphs or by removing whole pages or sections prior to the release of the document. Redactions should not just be a blank space, it should be clear that redactions have been made to a document and the amount of information redacted should also be clear.

2. REDACTION PRINCIPLES

2.1. Redaction must never be undertaken on an original document. Employees must always make a copy of the original document(s), and perform the redaction on the copied version. The copy document must be saved as the same name as the original document with the word 'redacted' inserted in the title. Failure to follow this naming convention correctly on the original and redacted documents may result in accidental disclosure of the unredacted version, which could cause a data breach and may lead to disciplinary action.

2.2. The original document(s) will be retained (either in hard copy or electronic format) for the appropriate retention period as set out in the Retention and Disposal Guidance and Schedule.

2.3. When dealing with SARs that involve hard copy/paper records, those records must be scanned into the Council's system to be redacted electronically.

2.4. Redactions should be made using the software approved and supplied by IT Services, currently PDF Studio. Redactions on Microsoft Word and Adobe are not appropriate as they can be undone by the recipient. A user guide for the redaction software can be found on the IT Helpdesk by searching for "redaction".

2.5. Within the current redaction software provided, it is not sufficient simply to use the redaction tool (under the Document Tab on PDF Studio) to highlight text to be redacted and then save it. You must then 'apply' the redactions and follow this up by 'sanitising' the document to remove any hidden data/metadata/comments/layers in the document. The sanitise function is accessed under Secure Tab>Sanitize on PDF Studio. Once the redactions are applied and sanitised, the document must be 'flattened' (under the Document Tab on PDF Studio) which prevents the redactions being undone. Failure to follow this process in full can lead to the redaction being left in a reversible state, or hidden data being accessible to the recipient.

2.6. Only the original version of the document(s)/data/information and the fully redacted version should be retained. Employees should not save a copy of the document with the redaction marks visible but reversible 'just in case' as this creates an increased risk that the wrong version of the document is disclosed or published. If the recipient queries or challenges the level of redaction carried out, comparison can be made between the original document

(completely unredacted) and the redacted copy document and if necessary, the challenged sections can be redacted again and disclosed or republished.

2.7. The redacted document/data/information should be converted into a pdf format (using the redaction software) prior to publication or disclosure to prevent carryover of any tracked changes which may allow reversal of the redaction and to prevent unauthorised alteration of the end document by the recipient.

2.8. When redacting data/information from electronic files/documents, you must ensure that there is no hidden data within the file document (e.g. hidden columns/rows or even worksheets on an Excel spreadsheet, white coloured text on a Word document, embedded documents or files within another document etc.). However, conversion to a pdf document, as per 6.7 above, may not completely remove hidden data, which could then be copied and pasted back into a Word Document to enable it to be seen. Care must be taken to ensure that all data (including hidden data) is checked and redacted (or removed if appropriate) before the data/information is published and disclosed.

2.9. When considering the withholding or disclosure of information under UK GDPR/DPA 2018, FOIA 2000 and EIR 2004 there is an obligation to communicate as much of the requested information as possible. As a result, blanket exemptions or exceptions to a whole document being disclosed/published will not normally apply or be lawful. The council can only withhold the whole document or data set when all the data/information contained within is exempt or excepted from disclosure or publication.

2.10. Redaction is normally carried out to remove words, sentences or paragraphs, but if so much information has to be redacted to that a document becomes unreadable, it may be appropriate to withhold individual sections, pages or even the entire document. However, if a document needs to be so heavily redacted, but there is information that is relevant and still makes sense after redaction; it may be more appropriate to type the unredacted information out separately or reference it in the response to the disclosure request or at the outset of publication of the data/information.

2.11. A whole sentence or paragraph should not be redacted if only one or two words are non-disclosable, unless release would place the missing words in context and make their content or meaning clear, or allow an individual to be identified either from the context of the sentence or in conjunction with wider information available elsewhere in the disclosure document(s).

2.12. It is important that redactions made to any data/information are consistent and logical, so that if a word is redacted in one part of the document for one reason, if that reason could apply to other text, redactions are also made to the other text based on that same reasoning.

2.13. Be clear on what data falls within the scope of the request you are dealing with, just because you have access to information does not mean you are authorised to disclose that information or that it falls within the scope of the request. Examples of this include:

- Information you hold on behalf of another organisation or third party;
- Information you have access to through a shared system.

If any of the above scenarios are applicable then the requester should be sign posted to the relevant organisation or third party for the information.

2.14. After all the information has been redacted from the physical document, it must be checked to ensure all the redacted information is unreadable and that the redaction cannot be undone.

2.15. The following information does not normally require redaction:

- Information originally provided by the requester, or parties in legal proceedings;
- Information previously provided to the requester/parties, except where information was provided to them in error;
- Information already known by the requester/parties;
- Information generally available to the public.

2.16. Where you are disclosing data/information in response to a SAR, you must prepare a schedule of documents that are being disclosed, including what information you have redacted and why.

2.17. Above all, if you are in any doubt about whether information should be redacted seek advice from your directorate IG Champion, the Information and Improvement Team (where in relation to a SAR, FOI or EIR request), the Information Governance Team or Legal Services.