

Children's Social Care Division

Subject Access Request (SAR)

Guidance Notes

1. Introduction

Subject Access Requests (SARS) are co-ordinated by the Information Governance Team and issued to the various Divisions. The designated Head of Service, currently Head of Service for Adolescent and Safeguarding, tracks and oversees the SAR completion process, and acts as a point of contact.

Work undertaken on a SAR must be carried out in accordance with the Corporate Subject Access Request (SAR) Policy.

2. Process for allocation of SAR work.

On receipt of the SAR from the Information Governance Team, the Head of Service, Adolescent and Safeguarding, will ensure/complete a check of MOSAIC (client database) to verify the case's current status.

- **If the child's case is currently open** to a Children's Social Care team, the Head of Service will notify the relevant Head of Service of the request and inform the Information Governance Team of the contact details of the current team e.g. Social Worker, Team Manager, Business Support Manager and Head of Service, to enable the Information Governance to forward the request to the relevant team. The Head of Service for the child's case will allocate the SAR within their service area and be accountable for the completion and quality assurance of the work. The Business Support Manager will allocate resource within the business support team for the service area, and oversee the work to redact documents.
- **If the child's case has been closed to a Children's Social Care team within the last 6 months**, the Head of Service will notify the previous Head of Service of the request, and inform the Information Governance Team of the contact details of the relevant service area and Head of Service, to enable the Information Governance to forward the request to the relevant team.

A "recently closed" case is taken to be a case where there has been a completed single assessment or further work within the 6 month period- If there has also been been an NFA referral, contact record or triage within the 6-month period, the SAR will still be allocated to the service area

that completed the substantive work with the child/young person. If there has only been a NFA referral, triage or contact in the last 6 months, the SAR will be treated as a closed case, as per below.

The Head of Service for the child's case will allocate the SAR within their service area, and be accountable for the completion and quality assurance of the work. The Business Support Manager will allocate resource within the business support team for the service area, and oversee the work to redact documents

The Head of Service for Adolescent and Safeguarding will create a rota for the allocation of SAR requests on cases that have been closed for more than 6 months. The rota will include all service divisions, and be held and monitored by the Head of Service, Adolescent and Safeguarding.

If there are resource/practice reasons why a service area is unable to complete work on a SAR allocated through the rota process, the relevant Head of Service will negotiate with colleagues for an alternative service area to undertake the SAR, or swap a slot, and will inform the Head of Service for Adolescent and Safeguarding of the new arrangement.

- **If the child's case has been closed for longer than 6 months**, on receipt of the SAR request from the Information Governance Team, the Head of Service for Adolescent and Safeguarding will identify the service area next on the SAR rota. They will notify the relevant area's Head of Service of the request and inform the Information Governance Team of the contact details of the relevant service area and Head of Service, to enable the Information Governance to forward the request to the relevant team. The Head of Service for the designated service area will allocate the SAR within their service area and be accountable for the completion and quality assurance of the work. The Business Support Manager will allocate resource within the business support team for the service area, and oversee the work to redact documents.

3. Downloading Documents and Attachments

The allocated worker undertaking the SAR will download documents from the following areas of MOSAIC:

- Documents (including all attachments)
- Case Notes

This will include all documents including letters and forms and may be undertaken in conjunction with business support- see **Appendix A**

4. Third Party Information

From the downloaded documentation any third-party information must be redacted (refer to Corporate SAR Policy) and to the SARS checklist (**Appendix C**) for

guidance (Corporate SARS Policy). If this task is undertaken by an appropriately trained business support member of staff, the work must be checked and agreed by a social work qualified member of staff.

Examples of third-party information include-

- Police (e.g. police notifications)
- Other Local Authority
- NHS/GP (e.g. health assessments)
- Education (e.g. school reports, school updates for reviews, etc)
- 3rd part is anyone other than the individuals that have not given their permission for their information to be included in the SAR request.

5. Redactions

Where the case is open or recently closed it is best practice for a discussion to take place with the social worker, Team Manager or IRO as part of the redaction process in order to be alert to any particular vulnerabilities in the case. However, any consideration not to share information which may be relevant needs to be discussed and agreed with the overseeing Head of Service and the Information Governance team.

Refer to the redaction guidance (**Appendix B**) for further information

- Always redact a copy not the original.
- Only use redaction when a few words, a sentence, a name or a paragraph need to be removed – consider providing a summary if most of a page is affected.
- Redaction should be carried out by knowledgeable and trained staff.
- Only redact what is exempt.
- Ensure redactions can't be reversed or decoded.

Methods:

- marker (mainly for small redactions)
- Nitro Pro

Consideration:

- Check carefully- and double check!
- Has information been redacted properly?
- Can the remaining information be disclosed?

6. Document Retention

- Retain three sets of documents as follows:

- Un-redacted version (full set of all documents)
 - Suggested redactions (copy prior to making all redactions permanent)
 - Redacted version
-
- Retain copies of documents for 3 years.
 - Current closed cases saved to [Safeguarding and Care Planning - Access to files - All Documents \(sharepoint.com\)](#)

7. Signing Off Completed SARs

On completion of the SAR work and carrying out the necessary redactions, the allocated CSC worker sends a link of the documents a nominated Team Manager to quality assure the work undertaken. When the team manager is confident that the work is correctly redacted, they send the link to a nominated Service Manager to sign off that they agree for the documents to be shared with the requestor.

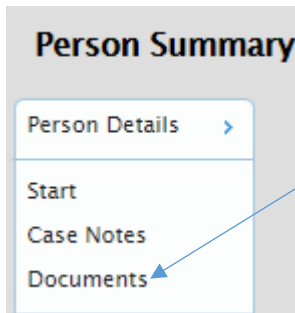
A covering letter sent in name of person signing off the SAR.

An email is sent to the Information Governance team, the overseeing Head of Service and the Head of Service, Adolescent and Safeguarding, confirming the date that the response was sent to the requestor.

Appendix A

How to access and download documents

Client's **Person Summary** screen select 'Documents'



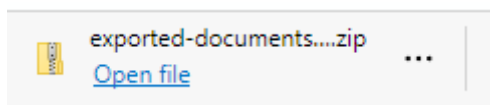
Sort in date order by sorting by 'Date'



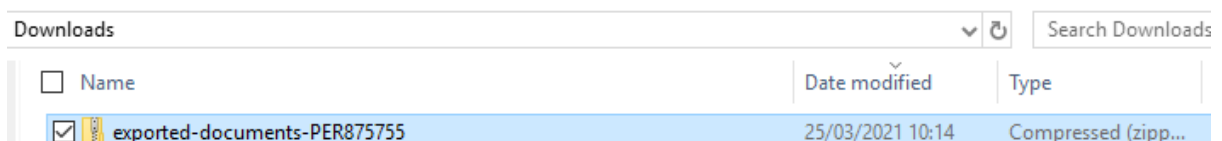
Scroll to end of document list and Select "Download All Forms and Letters"



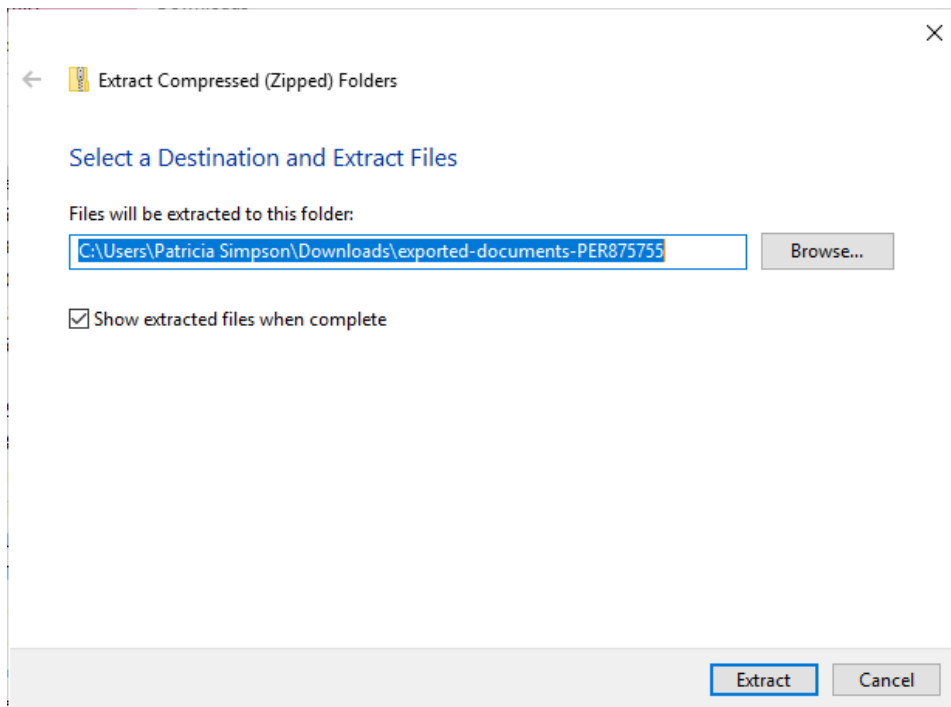
When documents are downloaded save a copy to a folder. Please note documents will be downloaded to a "zip folder".



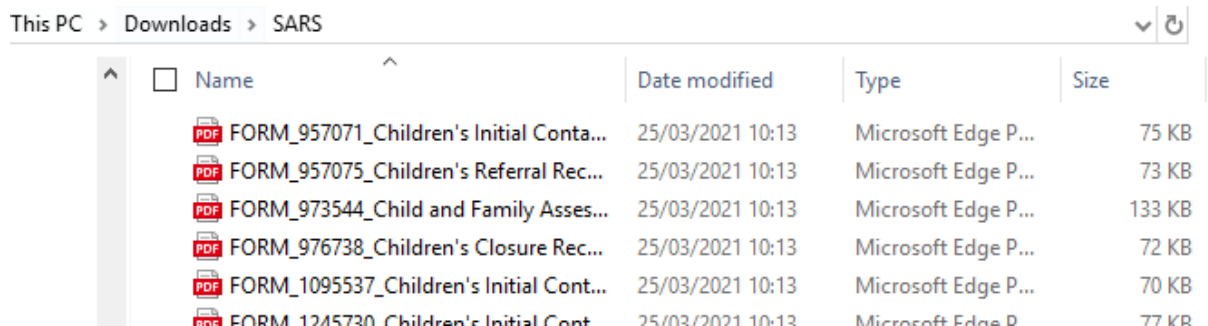
Go to "Downloads" folder and select the "zip" folder.




Right click and select “Extract All” and select “Browse” and save to folder of choosing



Create and name folder that documents will be saved to  Select “Extract”



Select the document to open in Nitro Pro by “Right Click”  Select “Edit in Nitro Pro”.

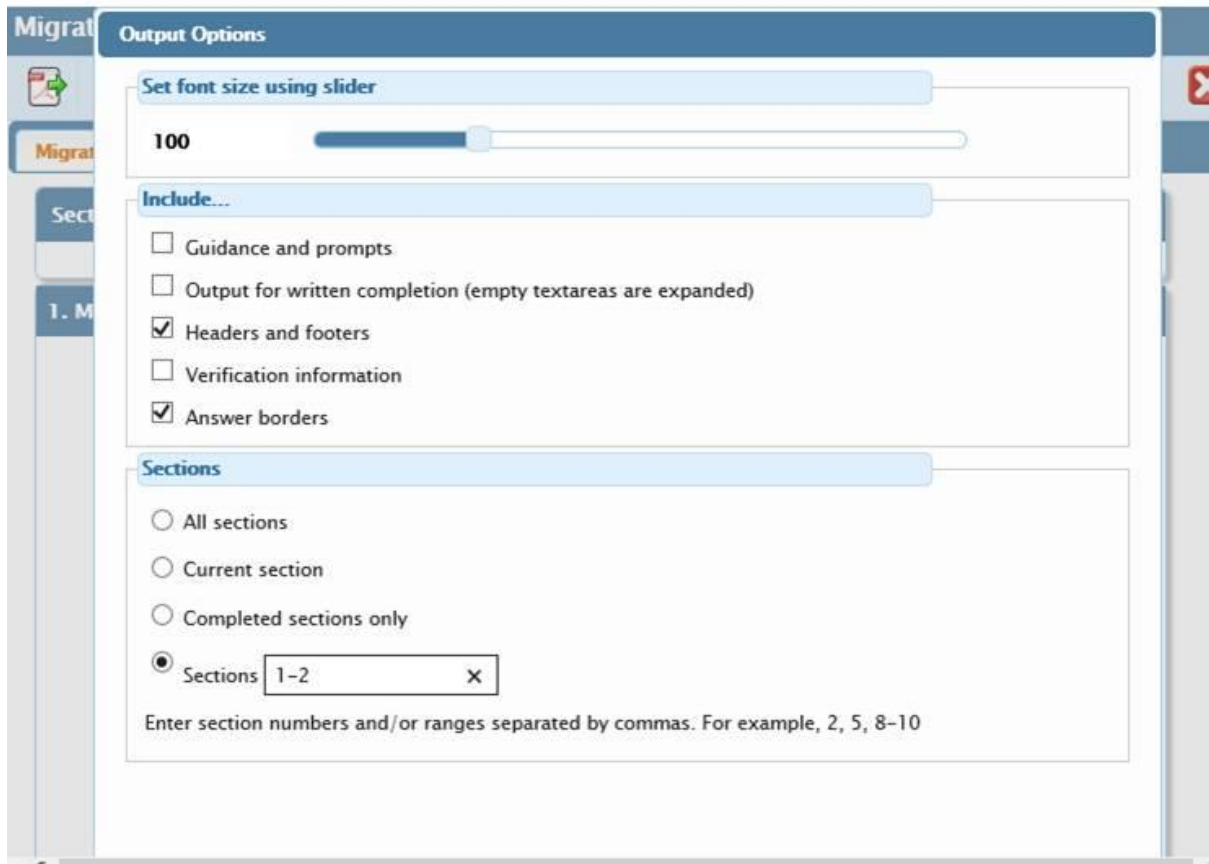
Documents are now ready to be redacted via Nitro Pro (please see sections on Redactions).

Opening individual migrated forms and removing blank pages

Select the PDF icon and open the document.

Open each form and select “Print to PDF” then save in numbered date order.

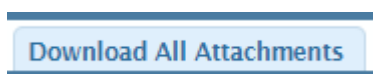
To exclude blank pages - select to print only sections 1+2 this avoids printing several pages of reportable fields with no added data as part of every form.



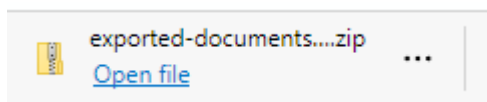
Next go to “Attachments” and download all attachments.



Select



Once documents have been down loaded save a copy to a folder. Please note documents will be downloaded to a “zip folder”.

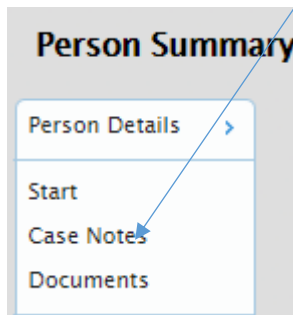


Select ‘Open file’ and save/export as required.

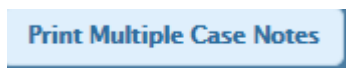
Open files in the saved location and follow the redaction instructions on how to redact documents using Nitro Pro.

Downloading Case Notes

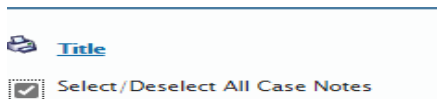
From Mosaic download all case notes records - Download all case notes by accessing "Case Notes" via the client's **person summary** screen



Select "Print Multiple Case Notes"



Select



Select > Print

Select from Printer Screen "**Microsoft Print to PDF**"

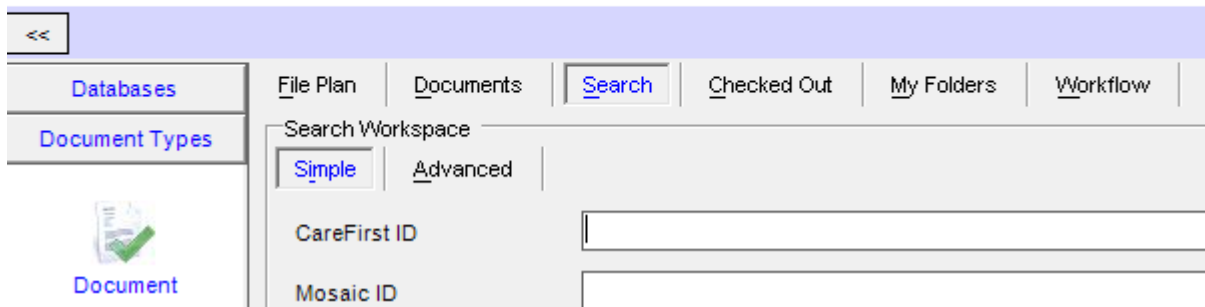
Select> Print>Rename file and save to Folder

Open files in saved location and follow redaction instructions on how to redact documents using Nitro Pro.

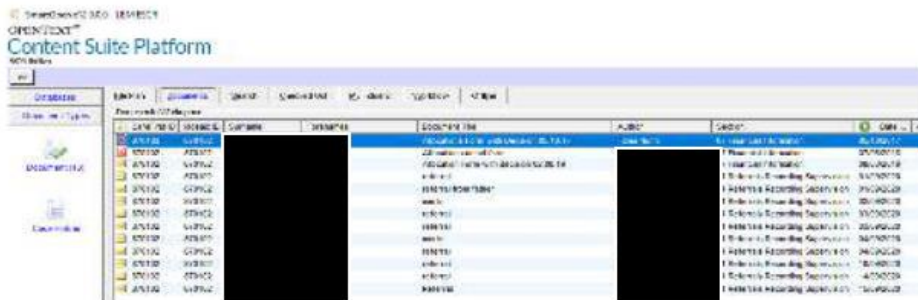
Downloading documents from LBM Smart

Open LBM Smart and download all documents. Open each document and attachment individually and save to a folder in preparation for redaction.

Search by "Mosaic ID"



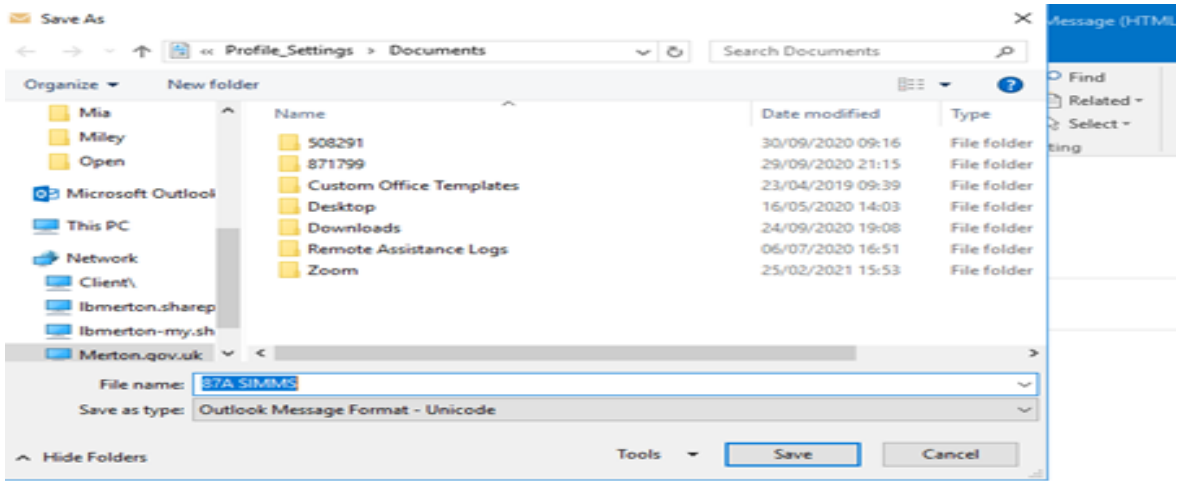
Right click on the item to be opened.



Select "Yes"



Then Select File from menu bar and select "Save As"



Useful Tips:

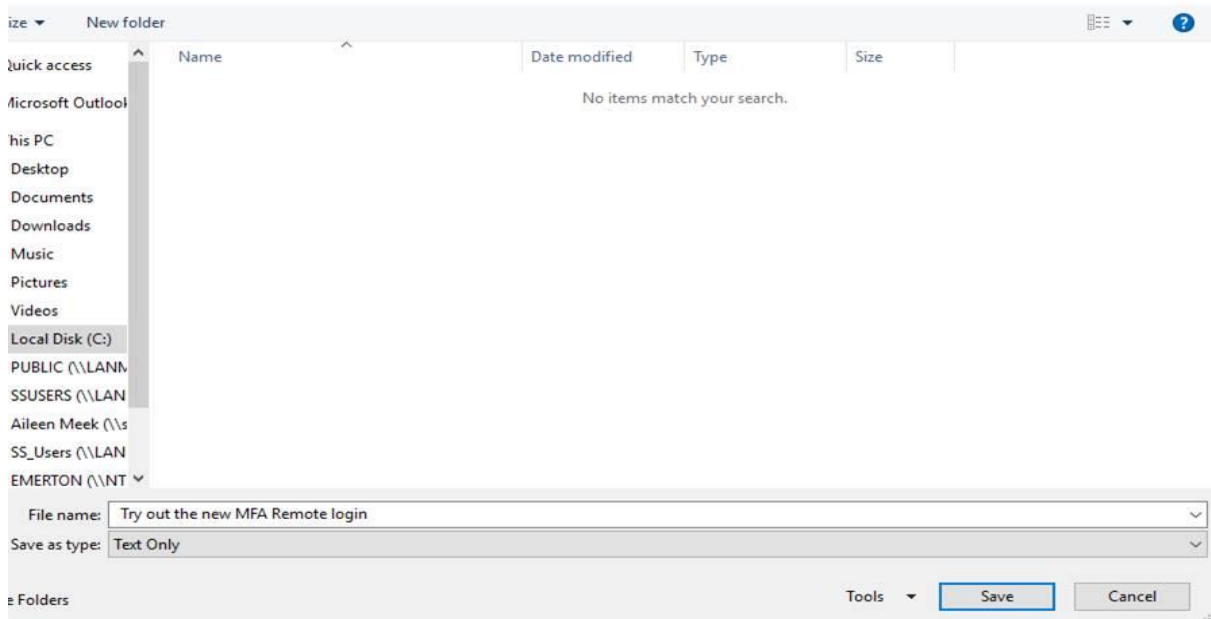
When saving documents - rename documents with a numerical pre-fix e.g. 001, 002, 003 and so on to ensure documents are saved in a numerical/chronological order.

Any Words document will need to be converted to PDF.

Use Nitro Pro to merge into one document following renaming individual documents numerically.

Downloading emails from LBM Smart

Open emails, forward it (so it has the headers available) and then save as “test only”. Any attachments are saved separately.



Useful Tip: (Saving to text can be useful when you have very long email trails which involve one or more sets of the 'this is a private email' gubbins which servers add.

Appendix B

Redaction

Redaction permanently removes parts of text or images from a PDF file and replaces them with black rectangles. This lets you remove sensitive information from a paragraph, table, heading, or a bitmap image. The rest of the document is unaffected, can be viewed, and printed normally.

Redaction is a two-step process — mark areas for redaction, and then apply redactions:

1. Select images, words, paragraphs, or pages, and apply redaction-marks. Redaction marks for text and images are non-destructive. They indicate which parts of the PDF document are selected for redaction.
2. When you are satisfied that all your redaction marks are suitably placed, and you want to permanently remove content marked for redaction, then you apply redactions.

NOTE: Redaction marks, images, and pages are removed permanently as soon as you apply redactions. Undo (Ctrl+Z) cannot restore redacted content after you Apply Redactions.

Redactions are not saved to the PDF document until you save the PDF file. If you apply an unwanted redaction, close the file immediately without saving, and re-open it.

When you save a PDF file with redactions, you are advised to use a different file name, and indicate that redactions are applied.

Redaction affects text and images on the content layer only. Therefore, if you want to remove an annotation or vector graphics, right-click it, and select Delete from the menu.

Mark for Redaction

To mark text for redaction:

1. On the Protect tab, click Mark Content, and select Mark for Redaction. The mouse cursor changes to an I-beam over text, an arrow over images, and a crosshair elsewhere.
2. Do one of the following:
 - Click and drag the I-beam cursor over text to mark parts of a word, words, or lines of a paragraph
 - Double-click the I-beam cursor to mark a single word

- Click and drag the crosshair cursor to mark a rectangular area

To mark an image for redaction:

1. On the Protect tab, click Mark Content, and select Mark for Redaction. The mouse cursor changes to an I-beam over text, an arrow over images, and a crosshair elsewhere.
2. Do one of the following:
 - Double-click the arrow cursor on an image to mark an entire image for redaction
 - Click and drag the crosshair cursor to mark a rectangular area

To mark pages for redaction:

1. Click the Pages tab on the left side of the window. The Pages panel opens.
2. In the pages panel, do one of the following:
 - Redact Page(s): Shift-click one or more pages to select them, and then right-click, and select Redact page(s)
 - Redact Page Range: Specify a range of pages to mark for redaction, and then filter by all, odd or even pages

To repeat marks across pages:

1. Right-click a redaction mark, and select Repeat Mark Across Pages
2. Specify a range of pages to receive the same redaction mark, and then filter by all, odd or even pages
3. Click OK to repeat the redaction mark in the same position on other pages

Remove a redaction mark

To remove a redaction mark, use the Mark for Redaction, Hand or Select tool, and do one of the following:

- Click on an area marked for redaction, and press Delete
- Right-click an area marked for redaction, and select Delete from the menu

Apply Redactions

To apply a redaction on an individual redaction mark:

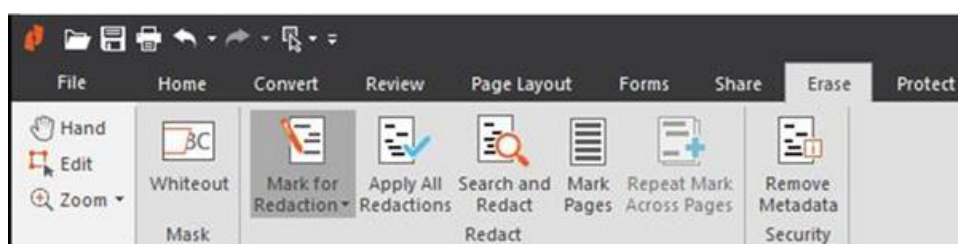
1. Right-click on the mark
2. Select Apply Redaction from the context menu

To apply redactions to all marked areas, do one of the following:

- On the Edit tab, click Redact, and Apply Redactions
- Ctrl+Shift+V

Remove Metadata Security

Complete and apply redactions and remove any metadata which can contain properties such as authors, document creation date, reference numbers, information about embedded images, etc



APPENDIX C

Subject Access Request checklist

Use this checklist before sending – http://intranet/data_protection-4

Do not send or redact original documents. If in doubt in relation to any aspect of a SAR please check with your line manager first and if further advice is needed contact the IG team.

To check	Done - Yes / No / N/A
Does the proof of identity proves who they are and that <u>the address you are sending to is correct</u> ? As well as photographic proof, a signature or knowledge of the address can be enough proof.	
Does the person have the right to request the information? If the child is over 12, can they, or have they, consented to their file being requested?	
Do you have all requested documents? Some requests are for specific documents, others are for a whole case file – however they may not be entitled to everything in that case file.	
Have you supplied all documents for the period requested?	
Have you searched for all electronic documents i.e. all drives and systems that your team use?	
Have you searched for all paper documents i.e. any that are stored in archives?	
If the amount of data is disproportionate, has the requestor been offered to view the data?	

Where information is about other members of the family does the requester know this information i.e. were they in attendance at meeting where information was discussed?	
If the requester is unaware of information about other family members, has it been redacted?	
Does the file contain whole documents about other family members? Unless requested and there is a right to the requested information about other siblings, documents wholly about other family members should not be sent out and should be filed in their own case file.	
Do the documents contain information about other cases? If yes then redact information about other case information – if the document has been misfiled, please file it correctly.	
Are council staff named in the documents requested and is the requester aware of their involvement i.e. attendee at meetings? If so redaction or consent is not required.	
Have you got consent from third parties to release their documents? Consent is required, unless the requester is aware of the third party document otherwise third party data must be redacted.	
Was the third party information given in confidence?	
Where Legal has provided information, have you checked with them what can be disclosed? Legally privileged information must not be released.	
Would releasing any of the information put the requestor or anyone else at risk of harm?	
Do the documents contain jargon etc.? You may need to explain these to the requester.	
If the requester is not collecting the information, are you sending it securely?	
Where have you kept a copy of all of the information sent?	
Name, signature and date completed	

Name of person completing checklist.....

Signature of person completing checklist.....

Have you carried out the protecting information training online and at what level?

Date checklist completed

Please keep a copy of this checklist with the copy of the information sent.

Please also save an electronic copy of this checklist with a note about where the information for the response has been saved

.....
.....