SUBJECT ACCESS REQUEST PROCEDURE

SPRING TERM 2025

DUE FOR RENEWAL: SPRING TERM 2027

CHANGES

November 2020	Policy implemented
January 2023	Policy reviewed, no changes made

CONTENTS

1. DEALING WITH A SUBJECT ACCESS REQUEST

Discovery MAT take our responsibilities and the data subject's rights of access to personal data seriously. This process ensures we meet our obligations and maintain the security of personal information during the process of gathering information requested.

2. INITIAL STAGES

Establishing the purpose of the request, particularly where the scope is very wide or complex, can assist the applicant to refine their request. This can make complying with the request more manageable for the Trust and result in the applicant receiving the information of importance to them without having to sift through voluminous records that the data subject is entitled to but has little or no interest in.

2.1 Initial Enquiries

2.1.1 When a data subject (or their parent/carer) makes an enquiry about accessing their personal data they should, in the first instance, be directed to the Data Subject Rights Request on the Trust website where they will find information about their rights of access and also the Trust's application form, if they wish to use it. Use of the Trust's form is not compulsory.

2.1.2 If the data subject wishes to make a verbal request, the scope of the request should be confirmed in writing on the verbal Subject Access Request Questionnaire (the requester should be sent a copy of this and given the opportunity to clarify if needed, when an acknowledgement is sent and (where necessary) identification is requested).

2.1.3 In most cases it will be beneficial to contact the requester to clarify the nature and scope of the SAR, the background to the request, options for how to receive the records and any ID or consent requirements.

2.1.4 When responding to an enquiry, due regard should be given to any disabilities or special needs the requester has and every reasonable assistance should be provided to support them in making their application.

2.1.5 Where the request is on behalf of a child or an individual without the capacity to make a request themselves we must establish that:

The requester has parental responsibility or

The requester is appointed by the court to manage the affairs of the individual and

Disclosure of the information is in the best interests of the child.

2.2 Verification of Identity

2.2.1 When a request is received a check is made to ensure that the appropriate consent and/or identification has been received. ID may not be required if the identity of the requester is known to the Trust. Where an identity check is required, two original documents from the following list are deemed to be appropriate identification:

☐ Birth certificate

☐ Divorce, annulment or separation document

☐ Marriage certificate

☐ Utility bill

☐ Passport

☐ Bank statement

☐ Medical card

☐ Letter from doctor, solicitor or probation officer

☐ UK residents permit

☐ Benefit or Tax Credit letter

☐ Pay slips

☐ Driving Licence

2.2.2 If a data subject or their representative is unable to produce any of these documents alternative means of confirming their identity should be discussed with them. This should then be referred to the DPO before any information is released.

2.2.3 Once sighted and recorded on our 'ID Confirmation Form', (appendix 1), documents received by post will be returned to the customer by recorded delivery.

2.2.4 Requester's are able to bring their identification into the Trust where their documents will be noted on the ID Confirmation Form and immediately returned to them.

2.3 Requests made on the Data Subject's Behalf

Where a third party submits a Subject Access Request on the Subject's behalf it's important to confirm that the third party is authorised to make the request. Subject Access Requests may be made about pupils, parents, staff, other adult visitors, etc.

2.3.1 Please see the Subject Access request policy for full details on how we will deal with requests made on behalf of children. An important point to note is that generally children over the age of 12 will need to provide their consent for a request to be made on their behalf, including by their parents.

2.3.2 In all instances where an application is made on a child's behalf the Trust needs to be satisfied that sharing the information is in the child's best interests.

2.3.3 Where the third party is a private individual, e.g. a friend or family member, identification should be requested for both the third party and the data subject along with written consent from the data subject authorising the third party to make the request.

2.3.4 Where the third party is a trusted non-statutory organisation (e.g. Citizen's Advice Bureau etc.) identification for the data subject and their written consent authorising the applicant to make the request should be asked for.

2.3.5 Where the third party is a solicitor's firm only the Subject's written consent is required to authorise the request.

2.4 Time for Compliance

2.4.1 It is important that the Trust establishes the deadline for responding to the request. This deadline is the latest that the information should be released, however, if it can be released sooner it

should be. This is a key date though and a calendar reminder should be added so that this is not missed.

2.4.2 The Trust has one month from the day that the application is received (whether or not this is a working day) to comply with the request. So if the request is received on 5th September the Trust has until 5th October to respond.

2.4.3 If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. For example if the request is received on 31st October the Trust has until 30th November to respond.

2.4.4 If the corresponding date falls on a weekend or a Bank Holiday, the Trust has until the next working day to respond. This is not the same as a 'Trust day' and the timescales apply even where the request is received or response is due, outside of term time.

2.4.5 If the request is large, complex or the Trust has received a number of requests from the data subject, the time for compliance can be extended by a further two months but the applicant must be notified within the first month with an explanation of why the extension is needed.

3. ADMINISTRATION

3.1 Allocation

When a request is received directly by the Trust this must be allocated to the Chief Executive Officer. The person dealing with the request will notify the DPO (if not already done) and complete the Subject Access Request Proforma, (see appendix 2). This will be the cover sheet to the case file, regardless of the file format.

3.2 File Format

According to the Trust's systems and preferences SAR case files can be set up:

- **A.** Both electronically and in hardcopy form. The hard copy case files will hold all of the personal data that has been requested. It will be kept in a wallet and stored securely in a locked cabinet with access restricted to the person dealing with the request. A copy of the application documentation and any ongoing communication in relation to the SAR should be scanned and saved in the electronic SAR case file. The individual electronic SAR case file should be established in the Executive folder in Sharepoint. Both files will be retained for the duration of the retention period set out in the data asset register and retention schedule.
- **B.** Both electronically and in temporary hardcopy form. The hard copy file will hold of the personal information until all of the information from all locations is together in one file. This will then be scanned as one pdf document for the purposes of electronic redaction and saved in the electronic SAR case file. The information in the hard copy file can be returned to its original locations. A copy of the application documentation and any ongoing communication in relation to the SAR should be scanned and also saved in the electronic SAR case file. The information in this file will be retained for the duration of the retention period set out in the data asset register and retention schedule.
- **C.** Electronic file only. If all records are already located electronically and the Trust no longer retains paper files then all of the information can be saved as pdf documents in the electronic SAR case file. A copy of the application documentation and any ongoing communication in relation to the SAR should be scanned and also saved in the electronic SAR case file. The

information in this file will be retained for the duration of the retention period set out in the data asset register and retention schedule.

The format that the SAR records are managed in and from which redaction occurs does not limit the format that the information can be sent to the requester. Electronic files can be printed for sending or collection and hardcopy files can be scanned for emailing. The requester has the choice of how they want to receive the information.

All requests should be logged on the SAR monitoring database – see section 4.

3.3 Assessment and Acknowledgement

3.3.1 An acknowledgement should be sent to the requester on receipt of the application. This should confirm how we will deal with the request and how long we have to deal with this. (See appendix 3)

3.3.2 The application should be reviewed at this time to ensure that all documentation has been provided and the needs of the data subject are fully understood.

3.3.3 If any documentation is missing or if any aspect of the request is unclear and we are unable to identify the requested information from the description provided we must notify the requester immediately. This must be included with the acknowledgement.

3.3.4 Where identification, clarification or consent is required, the Trust has 1 month from the date this is received to comply with the request. This should be confirmed in the acknowledgement.

3.3.5 Where only clarification of the request is required the person dealing with the request should try to telephone the requestor to establish the exact needs. They should use the telephone application form as a guide to asking for the correct information.

3.4 Locating and retrieving personal information

3.4.1 Where the information requested could be located in several locations, the person dealing with the request must send an email for all files and information to be passed to them in an agreed format within 2 working days. It is important that the information is collated quickly, giving enough time to organise the file, seek external views and redact relevant information.

3.4.2 An initial investigation should be made to see if there is any information held within the records that is not owned by the Trust. This may relate to social care reports, medical reports, e.g. from a doctor, counsellor or psychologist, other agency reports. If any such information is found we will contact the owner of the information to liaise about the release of this information (see appendix 4) and we will notify private foster carers (see appendix 4a). We will action this as a priority to enable a full response within the month time scale.

3.4.3 An initial skim read to highlight the documents which have been identified as relevant will also be undertaken. Depending on the file format a post-it or similar will be attached to each relevant record, or non-relevant documents will be placed in a holding folder in the electronic SAR case file in case they are deemed relevant at a later point. (Document relevance will be determined by the information requested in the initial application and, where appropriate subsequent discussion with the applicant).

3.5 Copying and printing (for file format options A and B)

3.5.1 Copying: Identified relevant information in the hardcopy file should be photocopied, single sided. During the photocopying process file security should be maintained and unauthorised access to the files prohibited. Copied material should be placed in date order in the clearly labelled wallet. The original file should be re-assembled and returned to its appropriate locked locations. When not in use the photocopied material should also be kept in locked storage.

3.5.2 Printing: Documents printed from electronic records should be co-located with the material copied from the hardcopy file. The storage wallet should be clearly labelled with its contents.

3.5.3 Scanning: Identified relevant information in the hardcopy file should be scanned to create an electronic pdf file. This should be organised in date order before scanning takes place so the scanned document is in the correct order. During the scanning process file security should be maintained and unauthorised access to the files prohibited. The original file should be re-assembled and returned to its appropriate locked locations.

3.6 Information security and storage

Security must be maintained at all times when the files are being worked on. The files should not be left unattended or accessible by unauthorised members of staff. All hardcopy files and print outs should be secured in locked storage when not in use.

3.7 Redaction (File format A)

3.7.1 Numbering the records: As the copy file or documents are read they should be systematically numbered using a light pencil mark in the top right hand corner of each sheet. This enables the continuity of the file to be re-established should pages be removed during the redaction process.

3.7.2 This should always be undertaken using the photocopy of the file/documents. **Originals must not be redacted.** Consideration should be given to whether any of the exemptions contained within the Data Protection Act 2018 might apply. Redaction should be completed by or under the guidance of the Data Protection Officer. Further details can also be found on the Information Commissioner's website.

3.7.3 How to redact: Redaction should be undertaken with a white correction roller. It is important that all redacted information is completely blanked out. For large blocks of redaction white sticky labels can also be used. When the redacted document is re-photocopied none of the redacted text must be visible.

3.7.4 What to redact: In general the redaction that will be required will relate to information about or provided by third parties. Examples of third party information includes information about the subject's relatives or reports about the subject provided by other agencies. Legislatively this will relate to Schedule 2, 3 and 4 of the Data Protection Act. Your Data Protection Officer can provide guidance on what information to redact. Further legislative guidance on the issue of third party information can be found on the Information Commissioner's website.

3.7.5 Coding Redactions: Reasons for redaction must be recorded on the file. Every time information is edited a relevant code number will be written against the information that has been removed, details of the redaction codes to be used can be found in (appendix 5).

3.8 Redaction (File format B & C)

3.8.1 Once the complete file is organised into an appropriate order in the electronic folder this information can be emailed, by secure email, to the Data Protection Officer for the purposes of redaction. The Data Protection Officer will collate all electronic records into one pdf file for the purposes of electronic redaction.

3.8.2 Coding Redactions: Reason for redaction must be recorded on the pdf file. Every time information is edited a relevant code number will be electronically selected against the information that has been removed, details of the redaction codes to be used can be found in (appendix 5).

3.8.3 Once satisfied that all text highlighted for redaction should not be disclosed and redaction codes have been added, redaction can be applied. The document should also be sanitised to remove any hidden data and metadata and flattened to prevent any redacted information from being re-established. The redacted file should be returned to the Trust by the Data Protection Officer.

3.9 Preparing the redacted file for disclosure

3.9.1 File Preparation - Hard copy redacted records should be photocopied, single sided. It is important to check that no redacted material can be seen in the photocopied records. The photocopied records will be checked to ensure that no un-related documents have been included. They will then be placed in an appropriate envelope/storage box. **A copy of 'Understanding Editing Codes' should be added to the file for sending (appendix 5).** A standard release letter will also be included, (appendix 6).

3.9.2 File Preparation - Electronic. Once the redacted file is returned to the Trust by the Data Protection Officer this should be saved in the SAR electronic folder. For clarity a sub 'disclosure' folder should be created and the file saved so it is easily identifiable as the 'redacted copy for disclosure'. **A copy of 'Understanding Editing Codes' should be added to the disclosure folder for sending** (appendix 5) A standard release letter will also be included, (appendix 6).

3.9.3 If third parties have been contacted to ask for any objections to the disclosure, we will include, full or redacted documents or fully exclude documents, in line with third party advice. [Note] the third party must have a relevant exemption in order to object to disclosure. If we are still waiting for third party views, we will advise the requester of this in the letter. The need to consult with third parties will not prevent the main body of our Trust records being issued to the requester. The outcome of discussions with the third parties will be sent to the requester in due course when a response has been received. This should still be within the one month timeframe.

3.9.4 When releasing records to the individual we must also confirm:

Our purposes for processing;

Categories of personal data we are processing;

Recipients or categories of recipient we have or will be disclosing the personal data to (including recipients or categories of recipients in third countries or international organisations);

Our retention period for storing the personal data or, where this is not possible, the criteria for determining how long we will store it;

The individual's right to request rectification, erasure or restriction or to object to processing;

The individual's right to lodge a complaint with the Information Commissioner's Office (ICO) or another supervisory authority;

Information about the source of the data, if it was not obtained directly from the individual;

The existence of automated decision-making (including profiling) and information about the logic involved, as well as the significance and envisaged consequences of the processing for the individual; and

The safeguards we have provided where personal data has or will be transferred to a third country or international organisation.

All of this information is contained in the Trust's privacy notice and therefore a copy of this can be included to satisfy the requirement to inform individuals of this information. The privacy notice to be included will be dependent upon who has requested the information and can be printed and added to the records if a hard copy is being provided. If records are being sent electronically a link to the privacy notice can be included in the email or an electronic copy added to the electronic disclosure folder.

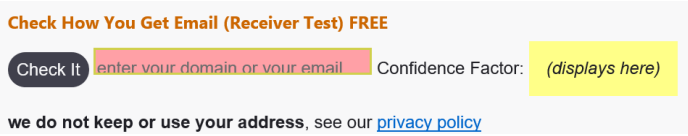
3.10 Releasing the file to the customer and case closure

3.10.1 Sending the hard copy file: The customer should be given the option of either collecting the files by hand or receiving them via Royal Mail Special Delivery – signed for. A record of the recorded delivery tracking reference should be held on the file (see appendix 7) and will be recorded on the log.

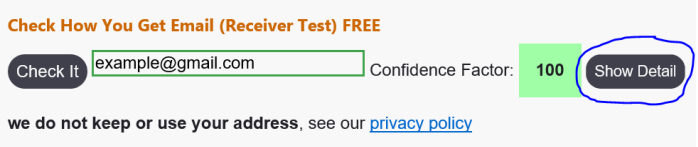
3.10.2 Collection: If the requester opts to collect the file by hand, they should bring appropriate identification, where required, (see appendix 1) and should be asked to sign the Release – Collection by Client Form, (see appendix 8).

3.10.3 Sending the electronic file: If the requestor has asked to receive their information electronically, the electronic file for disclosure, the standard release letter, the pdf version of 'Understanding Editing Codes' and the pdf version of the appropriate privacy notice (or link to the website), should be attached to an email with a covering message to state please find attached… If the collation and editing was completed in a hard copy format the file should be scanned to pdf and stored in the SAR disclosure folder and attached to an email as per the electronic file.

3.10.4 Security: Carefully check information is being sent to the correct address (postal or email) or is collected by the correct person before releasing any information. For electronic files, please ensure that the email address is secure. You can do this on-line at Check TLS. Scroll down until you see the section below and input the e-mail address you want to check in the red box and click the Check It button.



You will get a result as shown below and you can see further detail on the test by selecting the Show Detail button.



You would expect the confidence factor and all test results to be green, Ok and 100%.

If you have any concerns with the email address you are sending to, please refer to your IT department/provider or do not send personal or sensitive information by email to that email address. You should contact the requester to find an alternative way of releasing the information.

4. SUBJECT ACCESS – LOGGING REQUESTS AND MONITORING COMPLIANCE

Compliance with this policy and legislation will be monitored and details of this may be reported to the governing body at such time where this is deemed necessary.

Monitoring will capture:

The number of SAR's received;

SAR reference number;

Confirmation that appropriate identity checks were completed;

The date the request was received and the date it was responded to;

Whether the request has been actioned within the statutory time limit;

The reason for any delays past the statutory time limit;

Whether the data subject was informed of the delay and the reasons for this;

Whether the request was responded to within 3 months of receipt of the request (where a request is complex or numerous);

Details of the information provided;

Whether any information was withheld and the reason for this;

Whether a request was deemed unfounded or excessive and whether the data subject was adequately informed of the reason;

Whether a fee was charged;

Whether the data subject was informed of their rights to complain to the ICO.

Please see appendix 9 for an example of an appropriate monitoring log.

APPENDIX 1: ID CONFIRMATION FORM

ID check: For use on initial application and/or if file is being collected. Two documents from the following list constitute appropriate identification:

Birth certificate

Divorce, annulment or separation document

Marriage certificate

Utility bill

Passport

Bank statement

Medical card

Letter from doctor, solicitor or probation officer

UK residents permit

Benefit or Tax Credit letter

Pay slips

Driving Licence

Please note that original documents should be provided. Once copied the documents should be returned to the customer by recorded delivery.

Data Protection Act 2018 Confirmation of Identity

Client Name	
Proof of Identity	
Date Seen	
Staff Signature	
Staff Name	
Role	

APPENDIX 2: SUBJECT ACCESS REQUEST PROFORMA

Responsible Staff Member:	**Date:**

Data Subject Name	
Applicant Name (if different from above)	
Consent for third party to request information	
Description of information requested	
Date received	
Date Complete	
Action	
SIMS	
Trust's computer drive	
Trust's cloud storage	
Emails	
Laptops, Tablets or other portable devices	
Electronic child protection system (e.g. CPOMS)	
Electronic curriculum tools	

Paper Files	
No of wallets	

APPENDIX 3: ACKNOWLEDGEMENT LETTER TEMPLATES

– Choose from:

All information received

Dear <name of requester>

I am writing to confirm receipt of your request for access to your/name of data subject <*delete as appropriate*> records on <*insert date received*>.

Under the Data Protection Act 2018 we have one calendar month from the date that we received your request in which to respond. We will therefore deal with your request as soon as possible and issue a reply by no later than <*insert date received + 1 calendar month*>

Yours sincerely

All information received – verbal request

Dear <name of requester>

I am writing further to our conversation in which you requested access to your/name of data subject <*delete as appropriate*> records on <*insert date received*>.

Attached is a copy of my record of our conversation; please check that this is accurate and includes all of the information that you require. If you do need to clarify your request please let me know as soon as possible.

Under the Data Protection Act 2018 we have one calendar month from the date that we received your request in which to respond. We will therefore deal with your request as soon as possible and issue a reply by no later than <*insert date received + 1 calendar month*>

Yours sincerely

Additional information required (include relevant paragraphs)

Dear <name of requester>

I am writing to confirm receipt of your request for access to your/name of data subject <*delete as appropriate*> records on <*insert date received*>.

<*Unfortunately it is not clear what information you need and therefore to help us to deal with your request please could you provide further clarification of the information required.*>

<*As you are acting on behalf of <data subject name> we require their written consent before we can deal with the request. Please provide this to enable us to proceed. (Consider if ID is required for either or both parties and request this if needed)*

< *Before we are able to deal with your request we need to check your identity to ensure that you are legally able to make the request. Please provide two original documents from the following list:*

☐ *Birth certificate*

☐ *Divorce, annulment or separation document*

☐ *Marriage certificate*

☐ *Utility bill*

☐ *Passport*

☐ *Bank statement*

☐ *Medical card*

☐ *Letter from doctor, solicitor or probation officer*

☐ *UK residents permit*

☐ *Benefit or Tax Credit letter*

☐ *Pay slips*

☐ *Driving Licence>*

<Please provide this additional information as soon as possible. Under the Data Protection Act 2018 we have one calendar month from the date that we receive this information in which to respond.>

Yours sincerely

APPENDIX 4: DATA RELEASE LETTER

Dear

RE:<Data Subject Name> Date of Birth: XX\XX\XXXX

I am in receipt of a request for personal information under the Data Protection Act 2018 from <data subject>/agents name acting on behalf of <data subject> *(delete as appropriate).*

The enclosed documents form part of <data subject> Trust/staff (delete as appropriate) records. Please review the documents and let me know if you have any objections to the enclosed information relating to <data subject> being disclosed to <him/her/agents name> *(delete as appropriate*).

I would be grateful if you could respond, in writing, within **14 days** of receipt of this letter.

If you wish to discuss this matter further with me please do not hesitate to contact me on <telephone number>.

Yours sincerely

APPENDIX 4a: DATA RELEASE LETTER (FOSTER CARER)

Dear XXXXXX

RE:<Data Subject Name> Date of Birth: XX\XX\XXXX

The Trust has received a Subject Access Request in accordance with the Data Protection Act 2018 from XXXXXXXX(subject name/agent) who would like access to their Trust records.

These case records contains reports/assessments/recordings *(delete as applicable)* provided/made *(delete as applicable)* by foster carers from your organisation.

This information will be disclosed to XXXX (subject name/agent) on xx/xx/xx

Should you wish to have a copy of the information disclosed to XXXXXX (subject name/agent) or you have any other queries, please don't hesitate to contact me.

Yours sincerely

XXXXXXX

Data Protection Officer

APPENDIX 5: REDACTION – UNDERSTANDING EDITING CODES

Data Protection Subject Access Requests

Understanding Editing Codes Used in Your Records

When you make an application to have access to the information held about you, we'll ensure that you receive all of the information that you're legally entitled to see in accordance with your rights under GDPR and the Data Protection Act. Where information in your records is subject to exemptions contained in the Data Protection Legislation we're permitted to withhold it.

When you read the records we've supplied to you, you'll see that some of the information has been removed and replaced with a code number. These code numbers and the table below are designed to help you to understand why this information has been removed.

Whilst we've listed all of the exemptions that could apply to Trust records, however, there are two main reasons for editing information from your records, these are:

The information is not about you, it's about **another person**.

The information was supplied to the Trust by a professional worker not employed by the Trust. This worker would have been involved in your case. An example is a doctor or social worker. This is called a **third party view.** The Trust is required to ask the worker, or the organisation they work for, their consent to give you this information.

Editing Code Number	Legislation	Reason for Editing
-1-	Schedule 2, Part 3, Paragraph 16	**Data Protection Act Exemption – Protection of the rights of others.** The information relates to another person who can be identified from this information. The individual hasn't consented to the disclosure and it would be unreasonable to disclose this without their consent.
-2(1)-	Schedule 3, Part 2, Paragraph 6 (Restriction)	The information has been obtained from a professional working for another agency. **It is a third party view.** This includes Health data which we are restricted from disclosing as we are not health professionals and therefore require an opinion from a health professional to determine whether disclosure is appropriate. We are writing to the third party to ask for their view on whether to disclose this information to you.
-2(2)-	Schedule 3, Part 3, Paragraph 12 (Social Work)	**Data Protection Act Exemption – Opinion of Principal Reporter (Social Work)** This Social Work information has been processed by the Principal Reporter, in Scotland, in the course of their statutory duties. You're not entitled to receive this information from the Principal Reporter.
-2(3)-	Schedule 3, Part 4, Paragraph 20	**Data Protection Act Exemption – Opinion of Principal Reporter (Education)** This Education information has been

	(Education)	processed by the Principal Reporter, in Scotland, in the course of their statutory duties. You're not entitled to receive this information from the Principal Reporter.
Crime, law and public protection		
-3(1)-	Schedule 2, Part 1, Paragraph 2	**Data Protection Act Exemption – Crime and taxation.** This information has been processed for the purposes of the prevention and detection of crime; the apprehension or prosecution of offenders; or the assessment or collection of a tax or duty. We're unable to disclose this information if it would prejudice those purposes. We're, therefore, withholding this information whilst we write to the relevant law enforcement agency to ask for their opinion.
-3(2)-	Schedule 2, Part 1, Paragraph 3	**Data Protection Act Exemption – Crime and taxation.** This information has been processed for the purposes of the prevention and detection of crime; the apprehension or prosecution of offenders, or the assessment or collection of a tax or duty. We're withholding this information as disclosure would prejudice those purposes.
-4-	Schedule 2, Part 1, Paragraph 3	**Data Protection Act Exemption – Crime and taxation: risk assessment systems.** This information has been processed as part of a risk assessment system for the purpose of the assessment or collection of a tax or duty, the prevention or detection of crime or the apprehension or prosecution of offenders and cannot be disclosed as this would prejudice those purposes.
-5-	Schedule 2, Part 1, Paragraph 4	**Data Protection Act Exemption – Immigration.** This information has been processed for immigration purposes. This information cannot be disclosed as this would prejudice those purposes.
-6-	Schedule 2, Part 2, Paragraph 7	**Data Protection Act Exemption – Functions designed to protect the public.** This information has been processed for the purposes of protecting the public from malpractice and maladministration, to secure the health, safety and welfare of persons at work or others in connection with the activities of a person at work. This information cannot be disclosed as this would prejudice those purposes.
-7-	Schedule 2, Part 4, Paragraph 19	**Data Protection Act Exemption – Legal Professional Privilege.** This information consists of confidential communications between a client and their professional legal adviser for the purpose of seeking or giving legal advice, confidential communications between a client and their legal adviser (and also third parties) produced for the purpose of being used in actual or pending legal proceedings or other confidential communications between the client and professional legal adviser. This information cannot be disclosed.

-8-	Schedule 2, Part 4, Paragraph 20	**Data Protection Act Exemption – Self-incrimination.** This information would reveal that the Trust has committed a criminal offence and expose us to criminal proceedings. This information, therefore, cannot be disclosed.
Regulation, parliament and the judiciary		
-9-	Schedule 2, Part 2, Paragraph 10	**Data Protection Act Exemption – Regulatory functions relating to legal services, the health service and children's services.** This information has been processed for the purposes of a considering a complaint under Section 113(1) or (2), or Section 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003 or Section 24D or 26 of the Children's Act 1989. This information cannot be disclosed as it would prejudice those purposes.
-10-	Schedule 2, Part 2, Paragraph 14	**Data Protection Act Exemption – Judicial appointments, independence and proceedings.** This is information that has or is being processed by an individual acting in a judicial capacity, or a court or tribunal acting in its judicial capacity. This information cannot be disclosed as it would prejudice judicial independence or judicial proceedings.
Finance, management and negotiations		
-11-	Schedule 2, Part 4, Paragraph 22	**Data Protection Act Exemption – Management Forecasts.** This information has been processed for the purposes of management forecasting or planning and cannot be disclosed as this would prejudice the conduct of the relevant business or activity.
-12-	Schedule 2, Part 4, Paragraph 23	**Data Protection Act Exemption – Negotiations with the requestor.** This information records the Trust's intentions in respect of negotiations with the data subject and cannot be disclosed as this would prejudice the negotiations.
References and exams		
-13-	Schedule 2, Part 4, Paragraph 24	**Data Protection Act Exemption – Confidential References.** This information is a confidential references given or received by the Trust for the purposes of prospective or actual employment, education or training of an individual and cannot be disclosed.
-14-	Schedule 2, Part 4, Paragraph 25	**Data Protection Act Exemption – Exam scripts and exam marks.** This is the information recorded by the data subject in an exam, i.e. copies of answers to the exam questions and cannot be disclosed. Special rules apply to exam marks until the results are announced.
Journalism, research and archiving		
-15-	Schedule 2, Part	**Data Protection Act Exemption – Research and**

	6, Paragraph 28	**statistics.** This information has been processed for scientific or historical research purposes, or statistical purposes. This information cannot be disclosed as this would be likely to prevent or seriously impair achievement of the purposes of the research.
-16-	Schedule 2, Part 6, Paragraph 29	**Data Protection Act Exemption – Archiving in the public interest.** This information has been processed for archiving purposes in the public interest and cannot be disclosed as this would be likely to prevent or seriously impair achievement of the purposes of the archiving.
Health, social work, education and child abuse		
-17-	Schedule 3, Part 2, Paragraph 3 (Health) Schedule 3, Part 3, Paragraph 9 (Social Work) Schedule 3, Part 4, Paragraph 18 (Education)	**Data Protection Act Exemption – Health, Education and Social Work Records – data processed by a court.** This information has been supplied in a report or evidence given to a court in the course of proceedings and those proceedings are subject to statutory rules that prevent data from being disclosed to the data subject.
-18(1)-	Schedule 3, Part 2, Paragraph 4 (Health)	**Data Protection Act Exemption – Health data – an individual's expectations.** You've requested this information as someone who has (or is representing someone who has) parental responsibility for an individual aged under 18 or someone appointed by the court to manage the affairs of an individual without the capacity to do so themselves. This is third party information and the view of a Health Professional has been obtained (see code 2(1)). The view is that this information cannot be disclosed as the data subject would expect it to remain confidential.
18(2)	Schedule 3, Part 3, Paragraph 10 (Social Work)	**Data Protection Act Exemption – Social work data – an individual's expectations.** You've requested this information as someone who has (or is representing someone who has) parental responsibility for an individual aged under 18 or someone appointed by the court to manage the affairs of an individual without the capacity to do so themselves. This is third party information and the view of Social Care has been obtained (see code 2(1)). The view is that this information cannot be disclosed as the data subject would expect it to remain confidential.
-19(1)-	Schedule 3, part 2, paragraph 5 (Health)	**Data Protection Act Exemption – Health – serious harm.** This is third party information and the view of a Health Professional has been obtained (see code 2(1)). The view is that disclosure of this Health information would be likely to cause serious harm to the physical or mental health of the data subject or another person and, therefore, cannot be disclosed.

-19(2)	Schedule 3, part 3, paragraph 11 (Social Work)	**Data Protection Act Exemption – Social Work Records – serious harm.** This is third party information and the view of Social Care has been obtained (see code 2(1)). The view is that disclosure of this Social Work information would be likely to cause serious harm to the physical or mental health of the data subject or another person and, therefore, cannot be disclosed.
-19(3)-	Schedule 3, part 4, paragraph 19 (Education)	**Data Protection Act Exemption –Education Records – serious harm.** The disclosure of this Education information would be likely to cause serious harm to the physical or mental health of the data subject or another person and, therefore, cannot be disclosed.
-20-	Schedule 3, Part 5, Paragraph 21	**Data Protection Act Exemption – Child Abuse.** You have requested this information as someone who has (or is representing someone who has) parental responsibility for an individual aged under 18 or someone appointed by the court to manage the affairs of an individual without the capacity to do so themselves. This information is about child abuse and disclosure would not be in the best interests of the data subject.
Disclosure prohibited or restricted by an enactment		
-21-	Schedule 4, Paragraph 3	**Data Protection Act Exemption – Adoption Records and Reports.** This information consists of Adoption records and is subject to legislation which prevents its disclosure.
-22-	Schedule 4, Paragraph 4	**Data Protection Act Exemption – Statements of special education needs.** This information consists of an education, health and care (EHC) plan or information obtained in relation to the plan and disclosure is restricted by the Special Educational Needs and Disability Regulations 2014.
-23-	Schedule 4, Paragraph 5	**Data Protection Act Exemption – Parental order and reports.** The disclosure of this information is prohibited by regulations relating to the Adoption and Children Act 2002, the Human Fertilisation and Embryology Act 1990 and 2008, the Human Fertilisation and Embryology (Parental Orders) Regulations 2010, the Magistrates' Courts Act 1980 and the Courts Act 2003.
-24-	Schedule 4, Paragraph 6	**Data Protection Act Exemption – Information provided by Principal Reporter for children's hearing.** The disclosure of this information is prohibited by regulations relating to the Children's Hearings (Scotland) Act 2011 and the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013.
General		
-25-		**Out of scope of the request.** This information is not included in the access request and therefore does not need to be disclosed.

-26-		**Duplicate Information.** The information is a duplication of information provided elsewhere in the disclosure so has not been disclosed again.

The Information Commissioner's Office is the agency which regulates Data Protection in the United Kingdom. The Information Commissioner's Office website provides further, independent, advice on all aspects on Data Protection: http://ico.org.uk/

If you have any queries please do not hesitate to contact the Trust's Data Protection Officer.

APPENDIX 6: SUBJECT ACCESS REQUEST RELEASE LETTER

Standard Release Letter

Text in red is to be used with discretion when appropriate to the case.

Dear

Subject Access Request

Further to our recent contact I am pleased to enclose the Trust records that <name of Trust> hold for you *(or data subject's name if requester not subject).* As you will see, the documents have been edited. The Data Protection Act 2018 provides specific exemptions to information that cannot be included as part of your request. An example and the most common exemption applied, is information about other people. This means that I can only provide you with information that directly concerns you *(or data subject's name)*. I cannot supply personal information about other people including relatives.

The files also contain assessments and reports written by professionals outside of Trust, these are referred to as "third parties". The Trust needs to seek permission to release these documents to you and I have written to the following organisations asking for their consent to release documents to you:

Name of Organisation

Name of Organisation

As these organisations hold their own records, you may wish to make a Subject Access Request to them for all of the information they hold about you.

Court records withheld

The records that we hold about you contain information relating to Legal proceedings that you were the subject of / that you were involved in. As these documents belong to the court we are not able to disclose them. You can, however, make a request to the courts for these documents. Their contact details are….

I have attached a list of the abbreviations used within your files together with a list of the professionals referred to and the organisation they represented, which should help when you read through them. You will also find enclosed the document 'Understanding Editing Codes'. This explains why editing has taken place. As part of your request we must provide you with additional information about the data we are processing, for example, the category of information we process, the reason for processing and who we might share this with etc. This information is included in our privacy notice which I have also enclosed in this letter.

The policies, procedures and decisions that were made in the past are not *necessarily* standard practice today and decisions were made in the light of the circumstances and attitudes of those times.

Some of the information we have provided may be distressing to read, for example, details about your childhood which may conflict with what you already know. We would suggest that you have the support of another person when reading these records.

Some of the information is difficult to read due to the age of the records and because they are reproduced from a 'microfiche' film. A microfiche is a card made of transparent film used to store printed information in miniaturised form. Unfortunately, copies made from microfiche files do vary in their quality. You may also find that the papers aren't in date order and this will be because the original file was transferred to microfiche without being ordered.

Please can I remind you that the information enclosed is of a personal and sensitive nature and you are responsible for ensuring it is kept safe and confidential. Once you have finished with this information please ensure it is destroyed safely. If you wish you can return it to my office and I will arrange for it to be shredded.

If you should have any queries please do not hesitate to telephone me on the number at the top of this letter.

Yours sincerely,

XXXXX

Enc

Understanding Editing Codes

Copy: file

List of Abbreviations

Abbreviation	**Meaning**

List of Professionals

Name	Organisation

APPENDIX 7: ROYAL MAIL DESPATCH RECEIPT - SPECIAL DELIVERY

Tracked and Signed for

DISCOVERY MULTI ACADEMY TRUST

Serial Number	Name & Address

Despatched By: Date:

_____

Processed and despatched to Royal Mail

To track each mail item log onto www.royalmail.com

Enter the Serial Number into the Track & Trace box and press Track

APPENDIX 8: RELEASE – COLLECTION BY CLIENT FORM

DISCOVERY MULTI ACADEMY TRUST

T: <insert telephone number>

E: <insert email address>

Subject Access Request **Release of Information Form**	
Data Subject Name	
Details of Package	
Person Collecting	
Signature	
Proof of Identity	
Date Collected	
Staff Name	
Role	

APPENDIX 9: SUBJECT ACCESS REQUESTS LOG

														Was request deemed unfounded or excessive				
Reference Number	Date Received	How request was received	Date Acknowledged	Date consents sought from 3rd parties	Date Full response sent	Method of delivery: Postal (special delivery tracking number) / Collection (by whom)	Date 3rd party information sent (if different)	Identity checks completed	Response within statutory time limit	Was data subject informed of any delay and reasons for this?	For complex or numerous requests was a response sent within 3 months	Details of information provided	Details of information withheld and reason for this	Y/N	Reason	Was requester adequately informed	Was a fee charged and how much?	Was the requester informed of their rights to complain to ICO