Royton Hall Primary School

Data Subject Access Policy

Version 1
October 2019

1. Objectives

1.1. We recognise the need for legal compliance and accountability and endorse the importance of the rights of data subjects.

1.2. This policy sets out the key requirements in relation to the exercise of the individual right of data subject access to which we are fully committed.

1.3. These rights are different to rights of parents to have access to their child's education record under Pupil Information Regulations and have a different timescale - .See Appendix 3

2. Scope

2.1. In order to fulfil its statutory and operational obligations we have to collect, use, receive and share personal, special personal and crime personal data about living people, eg,

- Pupils and their families
- current, past, prospective employees
- clients and customers
- contractors and suppliers
- Governors members of the public (adults & children)

2.2. This policy covers the obligations to respond to data subject access rights in relation to personal data, regardless of data age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.

2.3. This policy reflects the commitment to data protection compliance to both UK and EU legislation, in particular the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR) and the EU Law Enforcement Directive 2016 (LED).

3. Policy

3.1. We will appoint a data protection officer who will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office.

Data Protection Officer

Justin Hardy
Data Protection Officer on behalf of Royton Hall Primary School:
West Street
Oldham
OL1 1UT

Email: DataProtectionOfficer@oldham.gov.uk
Tel: 0161 770 1311

3.2 General information: (see Appendix I for additional information)

3.2.1 As the Data Protection Act only relates to 'living' people, if a request is made for information on a deceased person seek advice from your line manager or the DPO. In this case we would still need to consider the duty of confidentiality owed to the data subject and others. Also, there may need to be consideration of other legislation.

3.2.2 There is no age bar on making a subject access request. It is possible that some children under 18 could be of an age and mental capacity to understand the nature of such a request and its implications and content. Generally speaking young people over the age of 12 are presumed to be of sufficient age and maturity to make a request in their own right. Equally, where an individual lacks mental capacity to make their own request, consideration needs to be on a case by case basis as to the legality of the request. Factors to consider are:

- who has legal authority in relation to the individual, e.g. legal parent, power of attorney litigation friend, etc?
- does the person have the capacity to understand the request and consent to it?
- would access to the personal data be in their best interest?
- could the disclosure cause harm to the data subject or anyone else

3.2.3 These requests may be made verbally or in writing.

If a request is made verbally and the applicant refuses or is unable to put it in writing, it would be good practice to provide the applicant with a written summary of your understanding of the request and ask them to confirm the summary is correct.

In all cases where there is any doubt as to the requestor's identity two proofs of identification will be necessary to confirm the requestor is who they say they are.

If ID and necessary information to locate requested information or to clarify what the requestor is asking, is not received then it may be necessary to 'lapse' the request if this is not received after 3 months.

Where a request is 'manifestly unfounded, excessive or repetitious' the law says we can either:

- Charge a fee to respond or
- Refuse the request on one or more of these grounds

As a matter of policy, where we determine a request is manifestly unfounded, excessive of repetitious we intend to refuse the request. Where we refuse a request the onus rests on us to demonstrate that the request falls within the threshold for relying on one or more of these grounds.

3.2.4 The final response should be made within one calendar month (in the case of pupil records 15 school days). See Appendix 3

The time starts the working day we are satisfied with verification of the data subject's identity and we have asked for and received sufficient information to process the particular enquiry.

This time can be extended to 2 calendar months where the case is complex or voluminous and the data subject has been informed of this within one calendar month of the original enquiry.

If an earlier request has been made within a timescale during which the information has not been significantly changed a repeat request may be refused.

3.2.5 As a minimum an individual has the right to know:

- what personal data is being processed
- the purposes why it is being processed
- the sources and recipients of the data
- whether the processing is outside of EU
- whether the processing involves automated processing or profiling
- their rights in relation to their personal data
- how to complain the council and /or the ICO

3.2.6 An individual is entitled to the information held about them; however, there are exceptions to this in very specific circumstances, but the starting point is from a presumption of disclosure. Seek advice from your line manager or the DPO – see Appendix 2.

3.2.7 The personal data needs to be provided in an intelligible format, the obligation is to provide the personal data and where possible copies of the documents that contain their personal data are the preferred means regardless of format

3.2.8 If the request relates to a process whereby an automated decision has been made e.g., recruitment, eligibility for benefits etc., the individual has the right to be given an explanation of the reasoning behind the automated process and request assessment to be undertaken by a person.

3.2.9 Data subjects are also able to:

- seek a review/complain to the DPO
- complain to the Information Commissioners Office (ICO)
- seek judicial remedy, including compensation through the courts

4. Assessment and Monitoring

4.1. An assessment of compliance with requirements will be undertaken in order to provide:

- Assurance
- Gap analysis of policy and practice
- Examples of best practice
- Improvement and training plans

4.2. Reports will be submitted to the Senior Management Team and Audit Committee.

5. Responsibilities and Approvals

5.1. **Governing Body**:

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2. **Head teacher**:

The Head teacher acts as the representative of the data controller on a day-to-day basis and is responsible for the approval of this policy.

5.3. **Data Protection Officer:**

The data protection officer will be the key contact for the provision of independent advice on all things data protection. The DPO will provide advice and support when dealing data subject enquiries and communications with the Information Commissioners Office

5.4. **Governors/Employees:**

All Governors and staff, whether permanent, temporary or contracted, including students, contractors and volunteers are responsible for ensuring they are aware of the data protection legislation requirements and for ensuring they comply with these on a day to day basis. Where necessary advice, assistance and training should be sought. Any breach of this policy could result in disciplinary action or could constitute a criminal offence

Appendix 1 – Process

Stage 1 – Recognition and receipt of a request

1.1 What is a request?

A data subject access request can be made verbally or in writing (paper, fax, email, social media, via websites), and does not need to state the legislation, or may indeed quote the incorrect legislation e.g. Freedom of Information.

The information we hold can be held in any format and be of any age. If it is clear that the request is for an individual's own data, then it needs to be responded to as a valid request under this process.

If a request is made verbally and the applicant refuses or is unable to put it in writing, it would be good practice to provide the applicant with a written summary of your understanding of the request and ask them to confirm the summary is correct.

In all cases (where there is any doubt as to the requestor's identity) two proofs of identification will be necessary to confirm the requestor is who they say they are.

Where a request is 'manifestly unfounded, excessive or repetitious' the law says we can either:

- Charge a fee to respond, or
- Refuse the request on one or more of these grounds

As a matter of policy, where a request is deemed manifestly unfounded, excessive or repetitious the option of a charge will not be offered and requests meeting these criteria will be refused. Where we refuse a request, the onus rests with us to demonstrate that the request falls within the threshold for relying on one or more of these grounds.

The only other circumstance where a modest administrative charge may be applied is in relation to a requestor seeking further copies of information supplied in response to a previous request. For requests that do not otherwise fall within the 'repetitious' category above, we may seek a charge and recover the costs of supplying additional copies.

If ID and necessary information to locate requested information or to clarify what the requestor is asking, is not received then it may be necessary to 'lapse' the request after 3 months.

It is essential that this type of request is recognised as falling under this process and the next step is to acknowledge the request under the correct legislation. If the request has been received via social media, it would be advisable to ask the individual for a separate and direct address for correspondence.

1.2 Logging /acknowledgment

All requests for subject access (SAR) need to be passed promptly to the school data protection lead for logging, acknowledgement, verification of request/seeking of ID etc and determining next steps.

It is good practice to clarify early within the calendar month that the request is being dealt with as a SAR under the DPA, and that the one calendar month, or extension to time applies.

The deadline begins when we are in receipt of:

- a valid request
- proof of identity
- proof of authority to act on data subject's behalf (where the request is made by third party)
- clear details of the records to be accessed

1.3 Request identification

It is important that we take all reasonable steps to ensure that the person making the request is entitled to make the request and receive access to the information. We must also establish whether or not it is full access to the records or specific information they are requesting.

Ways in which to validate a request made by the data subject:

- Personal knowledge of the applicant, e.g.by a member of staff involved with the applicant who can confirm they have the capacity to consent, Proof of identity, e.g. passport, picture driving licence or birth certificate, benefit or council tax notification along with utility bill or bank statement
- Comparison of signatures on file

Ways in which to validate a request made by an agent of the data subject:

- Signed consent from the data subject for the agent to act on the data subject's behalf
- Does the data subject have the capacity to understand the request being made?
- Is it in the data subject's best interest?
- Could the disclosure cause harm to the data subject or anyone else

1.4 Clarification and further information

If we do not have enough information to determine whether or not we hold the records, it may be likely that further detail may be required in relation to identification: e.g.

- proof of identity
- date of birth
- description of events/services received
- relevant time periods
- any proof of lawful authority to act on behalf of the data subject

1.5 Unstructured personal data

As the school is a public authority for the purposes of FOI, the processing of manual unstructured data ie, personal data that is not processed (or not intended to be) by automated ways and is manual data which forms part of structured filing system, is treated different within data protection law.

Unstructured Personal data is information **not included** in the following formats/contents

- held electronically
- stored in readily identifiable files structured by name and/or other identifiers

If the data is manual unstructured personal data and it relates to appointments, removals, pay, discipline, superannuation or other personnel matters then the obligations under data subject access around the provision of the data where we have been provided with a description of the data sought and it does not take more than 18hrs to determine if the data is held, and then locate, retrieve and extract the data.

Stage 2 –File preparation

2.1 Determine, locate, retrieve and extract

Although the easiest way to provide the relevant information is often to supply copies of original documents, you are not obliged to do so.

Once you have located and retrieved the personal data that is relevant to the request, you must communicate it to the requester in a clear and understandable way

In most cases, this information must be communicated to the requester by supplying him or her with a copy of it in permanent form i.e. hardcopy or electronic. You may comply with this requirement by supplying a photocopy or print-out of the relevant information or provide transcripts.

Ensure that any key abbreviations/coding/terminology is explained in the context of the information recorded.

Documents or files may contain a mixture of information that is the requester's personal data, personal data about other people and information that is not personal data at all.

This means that sometimes you will need to consider each document within a file separately, and even the content of a particular document, to assess the information they contain.

2.2 Consideration of exemptions

The Data Protection Act 2018 (DPA) recognises that in some circumstances you might have a legitimate reason for not complying with a Subject Access Request (SAR), so it provides a number of exemptions from the duty to do so. See Appendix 2.

Where an exemption applies to the facts of a particular request, you may refuse to provide all or some of the information requested, depending on the circumstances. It is a matter for you to decide whether or not to use an exemption – the DPA does not oblige you to do so, so you are free to comply with a SAR even if you could use an exemption.

It is not unreasonable to disclose the identities of a worker acting in an official capacity in delivering professional health, social care or education services

In cases, of unstructured personal data, where there is not a sufficient description of the data to enable its location and retrieval being carried out in less than the appropriate limit as set out in the Freedom of Information Act which is approximately 18 hours.

If manual records have been created or amended during the past calendar month the requestor must be offered an opportunity to view the records free of charge as they have a right to see them

2.3 Third party information

If the data subject's information contains the personal data of someone else and they can be identified, this information need not necessarily be provided to the data subject. To disclose a third party's personal data without consideration could lead to a breach of data protection.

Considerations include:

- Where this information relates to another individual, and has no association with the data subject e.g. is solely about the other person in their own right, it can be removed from the data to be provided
- Where the information is provided by another organisation

- Where the information has been provided by another individual about the data subject, or is about the data subject in association with another individual, it is possible to remove this, but only when considering:

  - whether or not the information could be anonymised to prevent the identification of others
  - if this is impossible, then consider seeking consent from the third parties to disclose
  - but… would seeking consent reveal that the data subject has made the request, has the data subject consented to this being made known?
  - when seeking consent ensure the person has a copy of what they are consenting to, be mindful of accidental disclosures when sending this, and set a deadline for response.
  - If consent cannot be sought, cannot be obtained, has been refused, or the request for consent has not been responded to then consider is it reasonable in all the circumstances to disclose the information without consent?
    - is there a duty of confidentiality to any of the persons identified e.g. would the information have been provided in an expectation of confidentiality, in relation to health, lawyer, financial, police, social worker, teacher, etc.?
    - Is there a public interest case in disclosing the information?
    - is the information already in the wider domain or known to the data subject?
    - is there a risk of harm to any parties or prejudice social work or detection and prevention of crime?

e.g., information provided by police, health, probation and/or any other non 'individuals' – seek consent, if not provided, remove and refer data subject to other bodies direct

e.g., minutes of a meeting attended by all the parties with all the information openly discussed – it would be reasonable to assume this reflected a situation that both individuals were aware of by being present at the meeting as participants. No need to remove the other individual's data

e.g., call from individual about the data subject. Information passed on as a confidential referral – either seek consent to disclose, if yes, then ok to disclose, if no or no response, anonymise or redact in order to preserve confidentiality, if this is impossible and the source could still be identified, then remove

2.4 Redaction

This is the process by which information can be removed but you must not alter or deface the original records. It is recommended that you either work on a copy of the information or replace selected original sheets with edited versions placed within the original file.

The removed, untouched, originals need to be kept with the file in a separate folder inaccessible to the data subject, (together with the consents correspondence and details of exempt information).

Redactions of information can be done in a variety of ways, depending on whether the information is electronic or paper. It could be:

- black markered out and re photocopied
- cut out and re-photocopied
- edited if electronic information
- It could be summarised and a digest of the information given

It is important that any redaction of information can be justified, and a record kept of what has not been disclosed and why

2.5 File letter

Ensure that a letter is prepared to outline the subject's record, as presented to them, e.g., whether or not a complete record, removal of third party information any exemptions, right to complain etc.,

Stage 3 – Information disclosure

3.1 Providing information

The information provided needs to be in an intelligible permanent form, e.g. photocopies, electronic files, prints outs etc. If the information contains codes or abbreviations the data subject should be advised what they mean. Also, where there may be difficulties in understanding the information provided, assistance should be given but this does not extend to translating into another language or typing up handwritten notes.

In exceptional circumstances the obligation to supply in permanent form does not apply. Firstly, where the data subject agrees otherwise, and secondly where it would be either impossible or disproportionate effort. It is the rarest of occasions that this would apply to, and consideration of accessing the information in another way, i.e., viewing and provision of some copies, needs to be made. Remember though the minimum requirements would still apply, i.e., a description of the data, the purposes why it is being processed, and to whom the data is being or may be disclosed.

3.2 Inform requestor information available/arrange delivery/collection

Inform the data subject the information is ready and arrange method of collection or delivery e.g.

- have them collect it from the school upon check of ID and sign a receipt
- have them organise courier
- fax or email only in exceptional circumstances and point out the risks to the data subject

Do not forget to:

- check you have the right details i.e., address, email, fax, etc.
- get a receipt from the data subject if possible and recheck ID
- keep a record of what is disclosed and what is not and why

3.3 Disclosure interview

In certain circumstances a service may offer a disclosure interview in order to support the request in upholding their information rights and the context

Stage 4 – Closure of request

The date the request has been completed the log should be updated and the original files to be returned to source together with a copy of the edited version provided to the applicant and the working file containing a record of the subject access procedure and decision making as to whether information was disclosed or withheld. This is important should any party have need to challenge the decisions to disclose or withhold information

Appendix 2 – Exemptions

These are the main exemptions that are likely to apply to data subject access requests, for full explanations please refer directly to the Data Protection Act 2018 together with guidance on the ICO website

These exemptions allow us to withhold information to the data subject

Schedule 2 Part 1

1 crime and taxation

Personal data processed for certain purposes related to crime and taxation is exempt from the right of subject access where disclosure would prejudice the following purposes:

• the prevention or detection of crime;
• the capture or prosecution of offenders; and
• the assessment and collection of tax and duty owed

5 required by law or in connection with legal proceedings

This exemption applies to personal data where it is either

a legal obligation to make public or disclose by law, an order of a court or tribunal:

or necessary for:

- actual/prospective legal proceedings
- the purpose of obtaining legal advice; or
- the establishing, exercising or defending legal rights.

In all cases, the discretionary exemption only applies to the disclosure to the extent that the disclosure would prevent compliance with that obligation.

Schedule 2 Part 2

16 protection of the rights of others

This provides an exemption from the right of access etc. to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information see section 2.3 for more information. In summary consideration of how reasonable it is to disclose a third party's personal data without consent.

19 legal professional privilege

This exemption applies where there is claim to legal professional privilege could be maintained in legal proceedings, or the information is subject to a duty of confidentiality between a professional legal adviser to a client of the adviser.

20 self incrimination

This exemption relieves a person from complying with the specified GDPR provisions to the extent that compliance would, by revealing evidence of the commission of an offence, expose the person to proceedings for that offence.

21 corporate finance
This provides an exemption for personal data processed for the purposes of or in connection with a corporate finance service to the extent that certain conditions are satisfied. This mainly relates to information which could adversely impact the orderly functioning of financial markets or the efficient allocation of capital within the economy.

22 management forecasts
This provides an exemption for personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned. An example might be reorganisation proposals prior to commencement of formal consultation.

23 negotiations
This provides an exemption for personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of those provisions would be likely to prejudice those negotiations.

24 confidential references
This provides and exemption for personal data references given in confidence for the purposes of education, training or employment, voluntary placement (including prospective)

25 exam scripts and marks
This provides an exemption for personal data consisting of:

(a) information recorded by candidates during an exam
(b) marks or other information processed by a controller—
- for the purposes of determining the results of an exam, or
- in consequence of the determination of the results of an exam

from the time limits for responding to access requests otherwise provided for in the GDPR which are replaced with time limits linked with the publication time table for the announcement of the results.

27 research and statistics
This provides an exemption for personal data processed for—

(a) scientific or historical research purposes, or

(b) statistical purposes

to the extent that disclosure would prevent or seriously impair the achievement of the purposes in question and where the resulting statistics do not identify the data subject.

28 archiving in the public interest
This provides an exemption for personal data processed for archiving purposes in the public interest to the extent that disclosure would prevent or seriously impair the achievement of the purposes in question and where the minimum personal data has been used and measures are in place to reduce the risk of personal identification, eg, pseudonymisation. Also, the processing does not cause the data subject substantial damage or distress or makes decisions in relation to individuals.

Schedule 3

2 health -data processed by a court
4 health -data subjects' expectations and wishes
5 health – serious harm
6 health -prior opinion of appropriate health professional
9 social work -data processed by a court
10 social work -data subjects' expectations and wishes
11 social work – serious harm
18 education -data processed by a court
19 education – serious harm
21 child abuse data

3, 9, 18 all relate to records processed by a court eg, information provided to court, evidence, part of proceedings etc. The court is able to withhold the information from the data subject

5, 11, 19 all relate to professional records which if disclosed would cause serious harm to the data subjects and/or others. The application of these exemptions has to be made by a health, social care, education professional

4, 10, where someone who has parental responsibility for someone under 18 or is appointed by a court to manage a data subject's affairs and makes a data subject access request, information may be withheld if the data subject has previously expressed that the information would not be disclosed to the requestors or where there would be a clear expectation of confidentiality.

6 if the information is health information, a data controller may not disclose this information unless the opinion of an appropriate health professional has been sought, unless the data controller is satisfied that the data subject knows or has seen the information.

21 where someone who has parental responsibility for someone under 18 or is appointed by a court to manage a data subject's affairs and makes a data subject access request, information may be withheld if the disclosure would not be in the interests of the data subject.

Schedule 4

3 adoption records and reports
18 statements of special educational needs
19 parental order records and reports

Prohibitions on disclosure exist for the provision of access to records via the data protection act 2018 data subject access rights.

Appendix 3 pupil information regulation requests (PIR)

A written request under pupil Information Regulations provides those with parental authority to receive a copy of child's educational records free of charge within 15 school days.

Information cannot be provided if disclosure via this regulation resulted in personal data being accessed that would not be permissible under the data protection act,nor would not be made available to the individual as part of a data subject access request.

http://www.legislation.gov.uk/uksi/2005/1437/contents/made

the ICO has a short guide that may be useful to you

https://ico.org.uk/your-data-matters/schools/pupils-info/

One of the key issues you would face is to determine what falls out of the PIR and what becomes a SAR. As a rule of thumb most information in relation to a child's school records would be covered by PIR unless there is information provided about the child from sources other than:

The child themselves
The parents
Education professionals/school staff