Whitegate End Primary School and Nursery

Individual Rights and Subject Access Request Policy

Responsible Committee	**FGB**
Date ratified	**25 June 2025**
Next review	**June 2027**
Signed	***K Painter***
Print name	**K Painter**

Contents

1 Introduction

1.1 The UK General Data Protection Regulations (UKGDPR) and Data Protection Act 2018 (DPA18) includes provisions for an individual to exercise a range of individual rights and have access to the personal information held about them. Whitegate End Primary School is recognised as a Data Controller under the Data Protection Act 2018.

1.2 Personal information is data that allows a living person to be identified from it, either from a single piece of data or alongside other data likely to come into our possession.

1.3 There are data protection principles that form the framework for managing personal data. These are detailed in the Data Protection Policy.

2 Individual Rights

2.1 Data subjects have the following rights: (see Appendix I for more information)

- The right to be informed
- The right of access (Subject Access Request or SAR)
- The right to rectification*
- The right to erasure*
- The right to restrict processing
- The right to data portability**
- The right to object**
- Rights in relation to automated decision making and profiling
- The right to be informed in the event of a data security incident

Plus, 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

Notes

** where the personal data needs to be retained for evidential purposes, the use of the information must be restricted from usage*

***the right to portability and objection does not apply to personal data for (LED) purposes*

2.2 As the Data Protection Act only relates to 'living' people, if a request is made for information on a deceased person, we would need to consider the duty of confidentiality owed to the deceased person and others. Also, there may be a need for consideration of other legislation such as where the request is in relation to a deceased person's health records, Freedom of Information amongst others.

2.3 There is no age bar on exercising an individual right or 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 is needed 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

2.4 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.

2.5 We will provide a written response within one calendar month that explains the outcome of our decision with regards to an individual query / request and / or complaint.

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. The target date is one calendar month after this date.

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.

2.6 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 one month.

2.7 In addition to requests that may be considered manifestly unfounded and excessive etc, as outlined in Section 4, there may be other reasons why it is not appropriate to provide the requested information fully or partly. A range of exemptions that could apply are outlined within Appendix II. These include:

- Rights of other individuals
- Crime and taxation
- Immigration
- Determined by law, and legal proceedings
- Other people's data unless consent, or reasonable without consent
- Confidential references

2.8 In relation to school records there are exemptions and variances in the legislation, policy and process– see Appendix II.

2.9 The response to the data subject needs to contain the following:

- Acknowledgement of the request / enquiry made
- Whether or not we are able to comply with the terms of the request and explanation of reasons / actions

- If we are unable to comply with what the request is seeking, an explanation of the reasons why.
- The right to complain to the ICO

3 Subject access request (SAR)

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

- what personal data is being processed
- the purposes of why it is being processed *
- the sources and recipients of the data *
- whether the processing is outside of the UK *
- whether the processing involves automated processing or profiling and an explanation as to the logic of the decision making and to request human intervention *
- their rights in relation to their personal data **
- how to complain the school and /or the Information Commissioner's Office (ICO) **

Notes

** This can often be provided by directing the individual to the appropriate privacy notice on the schools website*

*** This can often be provided by directing the individual to this Policy.*

3.2 A SAR should be responded to within one calendar month as outlined in 2.5. However, in respect of pupil records, parents have a right to request the educational record of their child under the Education (Pupil Information) Regulations 2005, which requires information to be provided within 15 school days. See Appendix IV for further information.

3.3 As outlined in 2.7 there are exemptions that could apply in very specific circumstances, but the starting point is from a presumption of disclosure– see Appendix II.

3.4 The obligation is to provide the personal data in an intelligible format and where possible, copies of the documents that contain their personal data. See Appendix III for further information on the process of handling a request.

3.5 It is an offence to make amendments or delete personal data in order to prevent its disclosure.

3.6 Records associated with SAR's should be kept and only kept for as long as necessary in line with appropriate retention periods.

3.7 An individual has the right to complain and to take the complaint to the ICO. Additionally, individuals have the right to seek remedy and compensation through the court process for material or non-material damages suffered as a result of non-compliance.

3.8 Enforcement notices, issued by the ICO, require organisations to take specified steps in order to ensure they comply with the DPA18. They can also issue monetary penalty notices, requiring organisations to pay up to £17.5 Million for serious breaches of data protection legislation.

4 Manifestly unfounded or excessive (MUE)

4.1 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

4.2 The following individual rights could be considered as manifestly unfounded or excessive

- The right of access (Subject Access Request or SAR)
- The right to rectification*
- The right to erasure*
- The right to restrict processing
- Rights in relation to automated decision making and profiling

4.3 The following factors should be considered when considering if a request is manifestly unfounded:

- the individual explicitly states, in the request itself or in other communications, that they intend to cause disruption;
- the individual makes unsubstantiated or false accusations against you or specific employees which are clearly prompted by malice;
- the individual is targeting a particular employee against whom they have a personal grudge;
- the individual makes a request but then offers to withdraw it in return for some sort of benefit from the organisation; or
- the individual systematically or frequently sends different requests to you as part of a campaign with the intention of causing disruption, eg once a week.

4.4 When considering if a request is manifestly excessive, we need to consider if the request is clearly and obviously unreasonable, taking into account if the request is proportionate and considering the burden on costs involved in handling the request.

4.5 When considering if a request is manifestly unfounded, excessive or repetitious, a MUE Assessment should be completed to outline the reasons why the request should be considered unfounded or excessive.

4.6 For cases where a request is considered as unfounded and/or excessive, the MUE Assessment should be approved by the Headteacher and the Chair of the Governing Body/Trust Board.

4.7 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.

4.8 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.

5 Complaints

5.1 Complaints relating to data protection will be managed in accordance with the school's complaints process with further advice and guidance sought from the DPO and / or School IG team.

5.2 We will adopt the following standards when handling complaints:

- We will refer to and use ICO guidance to help us respond to and deal with the issues raised
- We will do everything we can to resolve the issue to prevent escalation to the ICO
- If a complaint is raised with the ICO we will co-operate and demonstrate how we have complied with the law and identified where we can improve
- We will provide a detailed response to the customer including:
  - An explanation of the parts of the legislation that apply to their complaint in a way that's easy to understand.
  - If something has gone wrong, what we have done to put it right
  - If we have complied, then we've properly explained the parts of the legislation that allow us to process information in the way we have done
  - If there's more work for us to do, we will make this clear and provide an indicator of when they can expect to hear from us.

6 Implementation of policy

6.1 The Governing Body / Trust Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

6.2 The Headteacher acts as the representative of the data controller on a day-to-day basis and is responsible for the implementation of this policy.

6.3 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 Commissioner's Office.

Appendix I – Rights of Individuals

The right to be informed

Data subjects have the right to be informed about the collection and use of their personal data, this will primarily be via a privacy notice – (see the Data Protection by Design Policy and for more information)

The right of access

Data subjects have the right to request access to their own personal data and be provided with an intelligible permanent copy.

The right to rectification

Data subjects have the right to request the rectification of inaccurate or incomplete personal data. This request could be fulfilled by the provision of a supplementary statement. Where the personal data needs to be retained as part of the record, for evidence purposes, instead of rectifying it, its use could be restricted.

If you have shared/disclosed this personal data with another body, you must notify those recipients of the rectification/restriction of the information.

The right to erasure

Data Subjects have the right to be 'forgotten' but this does not apply in all circumstances.

It does apply where:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing
- you are processing the personal data for direct marketing purposes and the individual objects to that processing
- you have processed the personal data unlawfully
- you must do it to comply with a legal obligation
- you have processed the personal data to offer information society services to a child.

If you process data collected from children you should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

If you erase the personal data requested you need to notify any recipients you have shared/disclosed this information with, and if you have made the information public, then endeavour to remove it from the public domain/internet.

It does **not** apply in the following circumstances:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation
- for the performance of a task carried out in the public interest or in the exercise of official authority
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

In addition, the right does not apply to special personal data where:

- it is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- it is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

The right to restrict processing

Data Subjects have the right to request restriction/suppression of processing, but this does not apply in all circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. This may be an alternative to erasure or rectification, and it is unlikely that a restriction would be in place indefinitely but could be temporary whilst issues with the personal data are resolved. If you decide to remove the restriction you must tell the data subject **before** you continue to process the data**.**

The rights apply where

- the data subject contests the accuracy of their personal data and you are verifying the accuracy of the data
- the data has been unlawfully processed and the data subject opposes erasure and requests restriction instead
- you no longer need the personal data but the data subject needs you to keep it in order to establish, exercise or defend a legal claim
- the data subject has objected to you processing their data on grounds that you are relying on legitimate interests as your basis for processing, and you have no overriding legitimate interest to continue this processing or are processing it for profiling purposes.

Although this is distinct from the right to rectification and the right to object, there are close links between those rights and it would be good practice to automatically restrict processing whilst considering its accuracy and legitimate grounds of processing.

Ways of restricting processing may include, but are not limited to:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

The data should not be erased or changed whilst restricted and no further processing should take place during this time except to store it, unless:

- you have the individual's consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

If you restrict the processing of personal data, you need to notify any recipients you have shared/disclosed this information to.

The right to data portability

Data Subjects have the right to request for data portability, which allows data subjects to obtain and reuse their personal data for their own purposes across different services. This involves moving, copying, and/or transferring personal data easily across IT environments safely and securely

The right to data portability only applies:

- to personal data a data subject has provided to us;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

You must provide the data subject with their own personal data in a commonly machine readable form, eg, csv files. If the data subject requests it, and it is technically feasible, you need to transmit this data to another organisation. If the personal data concerns more than one individual, you must consider whether providing the information would prejudice the rights of any other individual eg, privacy, data protection, confidentiality etc

The right to object

Data subjects have the right to object to:

- Processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
  You must stop processing the personal data unless:
  - you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
  - the processing is for the establishment, exercise or defence of legal claims
- Direct marketing (including profiling);
  You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
- Processing for purposes of scientific/historical research and statistics.
  If you are conducting research where the processing of personal data is necessary for the performance of a public interest task, you are not required to comply with an objection to the processing.

Rights in relation to automated decision making and profiling

Data Subjects have the following rights where we make automated decisions about them or make decisions about them via profiling.

Automated decisions mean making a decision solely by automated means without any human involvement

Profiling means automated processing of personal data to evaluate certain things about an individual

This type of processing can only be carried out for decision making that is:

- necessary for the entry into or performance of a contract; or
- required by law; or
- based on explicit consent

The data subject should be informed as part of their privacy notice that this is taking place and the logic to the decision making process. They should also be advised how to request human intervention in the decision making process.

The right to be informed in the event of a data security incident which poses a high risk

Data subjects have the right to be informed if there is a serious data breach in relation to their personal data – see the Information security incident management policy for more information.

Appendix II – 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 3

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 In summary consideration of how reasonable it is to disclose a third party's personal data without consent.

Schedule 2 Part 4

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 UK 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 re-organisation proposals prior to the 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 UK 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, e.g., pseudonymisation. Also the processing does not cause the data subject substantial damage or distress or makes decisions in relation to individuals.

Schedule 3

3 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 III – 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. A Manifestly Unfounded/Excessive (MUE) Assessment should be completed prior to refusing a request.

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 one month.

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 B.

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 IV - Pupil information regulation requests

A written request under the Education (Pupil Information) Regulations 2005 provides those with parental authority to receive a copy of child's educational records free of charge within 15 school days.

In England, this right only applies to all local authority schools, and all special schools, including those which are not maintained by a local authority.

Independent schools, academies and free schools are not obliged to respond to a request for access to a pupil's education record under this legislation.

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, or 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. A PIR will likely cover information such as; the records of the pupil's academic achievements as well as correspondence from teachers, local education authority employees and educational psychologists engaged by the school's governing body.

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