Woolmore School
SCHOOL POLICY

Name	Data Protection Policy 2023-24 (including Subject Access Requests Procedure)		
Agreed by	Finance Committee		
Date agreed	February 2023	Review date	March 2024
Signed & dated			

Contents

1. Introduction

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

2. Definitions

2a Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for example, a name, email address, location or date of birth) or subjective (for example, an opinion about a person's actions or behaviour).

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved by reference to the individual or criteria relating to that individual.

2b Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

2c Data Subject

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

2d Data Controller

The organisation storing and controlling such information (i.e., Woolmore Primary School) is referred to as the Data Controller.

2e Processing

Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data; or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

2f Automated Processing

Automated processing involves any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

For example, automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

2g Data Protection Impact Assessment (DPIA)
DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

2h Criminal Records Information
This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

3. When can the school process personal data?

Data Protection Principles
The School is responsible for and adheres to the principles relating to the processing of personal data as set out in the GDPR. The principles the School must adhere to are set out below.

Principle 1
Personal data must be processed lawfully, fairly and in a transparent manner
The School will only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category of data as set out in the GDPR.

Before the processing starts for the first time we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data
The School may only process a data subject's personal data if one of the following fair processing conditions are met.

i) The data subject has given their consent.
ii) The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract.
iii) The processing is necessary to protect the data subject's vital interests.
iv) The processing is necessary to meet our legal compliance obligations (other than a contractual obligation).
v) The processing is necessary in order that we can perform a task in the public interest or in order to carry out official functions as authorised by law.
vi) The processing is necessary for the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The School may only process special category data if we are entitled to process personal data (using one of the fair processing conditions above) AND at least one of the following conditions is met.

i) The data subject has given their explicit consent.

ii) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay.

ii) The processing is necessary to protect the data subject's vital interests.

iii) The processing is necessary to meet our legal compliance obligations (other than a contractual obligation).

iv) The data has been made public by the data subject.

v) The processing is necessary to perform a task in the substantial public interest or in order to carry out official functions as authorised by law.

vi) The processing is necessary is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

vii) It is necessary for reasons of public interest in the area of public health.

viii) The processing is necessary for archiving, statistical or research purposes.

ix) The School identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

i) Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

ii) A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action relating to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

iii) Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

iv) If explicit consent is required, the School will normally seek another legal basis on which to process that data. However, if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

v) The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Principle 2

Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The School will only process personal data when our obligations and duties require us to. We shall not collect excessive data. We shall ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete, destroy or anonymise the data. Please refer to the School's Data Retention Policy for further guidance.

Principle 4
Personal data must be accurate and, where necessary, kept up to date

The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification of incomplete or inaccurate data held by the School.

Principle 5
Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that we adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Data Retention Policy for further details about how the School retains and removes data.

Principle 6
Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as the following.

i) Encryption

ii) Pseudonymisation (This is a process by which the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.)

iii) Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it.)

iv) Adhering to confidentiality principles

v) Ensuring personal data is accurate and suitable for the process for which it is processed

The School follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place, including, but not limited to, the following.

i) The School has established that the third party has a need to know the information for the purposes of providing a contracted service.

ii) The sharing of personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;

iii) The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place.

iv) The transfer complies with any applicable cross border transfer restrictions.

v) A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities – for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals with a third party body will be clearly defined within written notifications and details of and the basis for sharing that data will be given.

Transfer of Data Outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

The School will not transfer data to another country outside the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School's guidelines on transferring data outside the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

4. Data Subjects' Rights and Requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data. The rights data subjects have in relation to how the School handles their personal data are set out below.

i) (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time

ii) To receive certain information about the School's data processing activities

iii) To request access to their personal data that we hold (see "Subject Access Requests" at Appendix 1)

iv) To prevent our use of their personal data for marketing purposes

v) To ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data

vi) To restrict processing of data in specific circumstances

vii) To challenge data processing which has been justified on the basis of our legitimate interests or in the public interest

viii) To request a copy of an agreement under which personal data is transferred outside the EEA

ix) To object to decisions based solely on automated processing

x) To prevent processing that is likely to cause damage or distress to the data subject or anyone else

xi) To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms

xii) To make a complaint to the supervisory authority

xiii) In limited circumstances, to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

Direct Marketing

The School is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls). The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

Employee Obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must:

i) only access the personal data that you have authority to access and only access it for authorised purposes;

ii) only allow others to access personal data if they have appropriate authorisation;

iii) keep personal data secure (for example, by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction (please refer to the School's Security Policy for further information about our security processes);

iv) not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information;

v) not to store personal information on local drives.

5 - Accountability

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles. The School has taken the following steps to ensure and document GDPR compliance.

a) Appointing a Data Protection Officer (DPO)

The School has appointed Judicium Consulting Ltd to undertake the duties of a Data Protection Officer. The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Their contact details are:
Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203-326 9174
Lead Contact: Craig Stilwell

If you have any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed, please contact the School Business Manager, who is responsible for the day to day operation of this policy in School. If this does not resolve the matter, you should then contact the Data Protection Officer. In particular, you must always contact the DPO in the following circumstances.

i) If you are unsure of the lawful basis being relied on by the School to process personal data;
ii) If you need to rely on consent as a fair reason for processing (please see above the section on consent for further information);
iii) If you need to draft privacy notices or fair processing notices;
iv) If, having consulted the School's Data Retention Policy, you remain unsure about the retention periods for the personal data being processed;
v) If you are unsure about what security measures need to be put in place to protect personal data;
vi) If there has been a personal data breach (in which case, you should also have regard to the School's Breach Notification Policy;
vii) if you are unsure on what basis to transfer personal data outside the EEA;
viii) If you need any assistance dealing with any rights invoked by a data subject;
ix) whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
x) If you plan to undertake any activities involving automated processing or automated decision making;
xi) If you need help complying with applicable law when carrying out direct marketing activities;
xii) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

b) Personal Data Breaches

The GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO). We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator when we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. You should Immediately contact School Business Manager, who is the person designated as the key point of contact for personal data breaches, or your DPO.

c) Transparency and Privacy Notices

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices [and/or Fair Processing Notices] which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy Notices set out information for data subjects about how the School uses their data and the School's Privacy Notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This will be provided in our privacy notice.

When personal data is collected indirectly (for example from a third party or publicly available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also advise the data subject whether that third party has collected and processed data in accordance with the GDPR.

Notifications will be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

Privacy By Design
The School has adopted a privacy be design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

Data Protection Impact Assessments (DPIAs)
In order to achieve a privacy by design approach, the School will conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the GDPR in the following circumstances:

i) for the use of new technologies (programs, systems or processes) or changing technologies;
ii) for the use of automated processing;
iii) for large scale processing of special category data;
iv) for large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain:

v) a description of the processing, its purposes and any legitimate interests used;
vi) an assessment of the necessity and proportionality of the processing in relation to its purpose;
vii) an assessment of the risk to individuals;
viii) the risk mitigation measures in place and demonstration of compliance.

Record Keeping
The School are required to keep full and accurate records of our data processing activities. These records include:

i) the name and contact details of the School;
ii) the name and contact details of the Data Protection Officer;
iii) descriptions of the types of personal data used;
iv) description of the data subjects;
v) details of the School's processing activities and purposes;
vi) details of any third party recipients of the personal data;
vii) where personal data is stored;
viii) retention periods;
ix) security measures in place.

Training
The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

Audit
The School regularly tests our data systems and processes in order to monitor compliance and to review the use of personal data. This is done through period checks made by the SBM and, more formally, by data audits which are carried out annually by the DPO.

Monitoring
The School will monitor the effectiveness of this Data Protection policy and all related policies and procedures. These will be reviewed annually or when the DPO advises this is necessary (for example, when legislation changes) and updated as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

Related Policies
Staff should refer to the school's set of policies which cover data protection and the GDPR and which are designed to protect personal data. These policies can be found with other school policies made available to staff. Staff should pay particular attention to the following policies, which are related to this Data Protection Policy:
Data Retention Policy
Security Policy
Breach Notification Policy and Procedures

6. Automatic Processing and Automated Decision Making

The School understands that automatic processing of data and automated decision making refer to activities such as using collected data (such as clocking in and out times or exam results) to trigger actions (such as punctuality warnings or allocation to classes) and where no human intervention is used in carrying out the evaluation of that data and the implementation of the consequences of it. The School does not carry out automatic processing of data or automated decision making and understands that if we begin to do so, we shall work with our DPO to insert a relevant section of policy at this point in our overall Data Protection Policy.

Name	Data Protection Policy 2022-23 Appendix: Subject Access Requests (SAR) Procedure

Contents

How to recognise a subject access request
Under Data Protection Law, Data Subjects have a general right to find out whether the School holds or processes personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data Subject Access Request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the School is undertaking.

A Data Subject has the right to be provided by the School with the following:
i) confirmation that their data is being processed;
ii) access to their personal data;
iii) a description of the information that is being processed;
iv) the purpose for which the information is being processed;
v) the recipients/class of recipients to whom that information is or may be disclosed;
vi) details of the School's sources of information obtained;
vii) in relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making; such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct;
viii) other supplementary information.

How to recognise a subject access request
A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child) to establish whether the School processes personal data about him or her and, if so:
i) for access to that personal data;
ii) and/or certain other supplementary information

A valid SAR can be made either in writing (by letter or email) or verbally (e.g., during a telephone conversation). The request may refer to the GDPR and/or to "data protection" and/or to "personal data" but does not need to do so in order to be a valid request. For example, a letter which states "please provide me with a copy of information that the School holds about me" will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request
While there is no requirement to do so, we encourage any individuals who wish to make a date subject access request to make the request in writing, detailing exactly the personal data being requested. This allows the School to recognise easily that the individual wishes to make a data subject access request and the nature of the request. If the request is unclear and/or vague, the school may be required to clarify the scope of the request, which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request
All data subject access requests should be immediately directed to the School Business Manager, who should contact the DPO (I.e., Judicium) in order to assist with the request and what is required.

Acknowledging the request
When receiving a SAR, the School will acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:
i) proof of ID (if needed);
ii) further clarification about the requested information;
iii) clarification of the address/email address to which the School should send the requested information (if it is not clear where the information shall be sent);
and/or

iv) consent (if the request is for third party data).

The School should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request
Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts about the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, a birth or marriage certificate, a credit card or a mortgage statement.

If an individual is requesting a large amount of data, the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. If more information is needed before the School can respond to the request, the School will let the requestor know as soon as possible.

In both cases, the period of responding begins when the additional information has been received. If the School does not receive this information, it will be unable to comply with the request.

Requests made by third parties or on behalf of children
The School needs to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

The School will assess whether the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, should take into account any relevant factors including, but not limited to:

i) the child's level of maturity and their ability to make decisions like this;
ii) the nature of the personal data;
iii) any court orders relating to parental access or responsibility that may apply;
iv) any duty of confidence owed to the child or young person;
v) any consequences of allowing those with parental responsibility access to the child's or young person's information (this is particularly important if there have been allegations of abuse or ill treatment);
vi) any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
vii) any views the child or young person has on whether individuals with parental responsibility should have access to information about them.

Generally, a person aged twelve years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child twelve years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will either require the written authorisation of the child before responding to the requester or will provide the personal data to the child direct.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee for responding to a SAR
The School will usually deal with a SAR free of charge. If a request is considered to be manifestly unfounded or excessive, a fee to cover administrative costs may be requested.

Time Period for Responding to a SAR
The School has one calendar month to respond to a SAR. This will run from the day on which the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received – whichever is the latest.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex to require an extension of the period for response, the School will need to notify the requester of the extension within one calendar month of receiving the request, together with the School's reasons why this extension is considered necessary.

School closure periods
The School may not be able to acknowledge a request received during or just before school holidays or other closure periods, or to respond within the one calendar month response period, because there may not be any appropriate staff on site to receive and deal with a request.

The School will endeavour to comply with requests as soon as possible and will keep the person making the request informed.

Information to be provided in response to a request
The individual is entitled to receive access to the personal data the School processes about him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing and will be provided in a commonly-used electronic format.

The information that the School is required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School has one month in which to respond, the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The School is, therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

How to locate information
The personal data the School needs to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Protection of third parties – exemptions to the right of subject access
There are circumstances in which information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious to whom the data relates), then the School does not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual

(including information identifying the other individual as the source of information) who can be identified from the information unless:

i) the other individual has consented to the disclosure; or
ii) it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, the School will take into account all of the relevant circumstances, including:

i) the type of information that would be disclosed;
ii) any duty of confidentiality the School owes to the other individual;
iii) any steps taken to seek consent from the other individual;
iv) whether the other individual is capable of giving consent; and
v) any express refusal of consent by the other individual.

In each case, the decision on whether to disclose the information will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard, the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

i) Crime detection and prevention
   The School does not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

ii) Confidential references
   The School does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:
   a) education, training or employment of the individual;
   b) appointment of the individual to any office; or
   c) provision by the individual of any service.
   This exemption does not apply to confidential references that the School receives from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

iii) Legal professional privilege
   The School does not have to disclose any personal data which are subject to legal professional privilege.

iv) Management forecasting
   The School does not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

v) Negotiations
   The School does not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Woolmore School
SCHOOL FORM

Name	Subject Access Requests Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of identity We require proof of your identity before we can disclose personal data. Documents we accept as proof of your identity include your birth certificate, passport, driving licence, official letter addressed to you at your address, bank statement, recent utilities bill andr council tax bill. If the name on your document is different from the name you now use because you have officially changed your name, we shall ask you to supply documentary evidence of the change.

Section 1
Please fill in the details of the data subject (i.e. the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own. Please write clearly.

Title	
Surname/ Family Name	
First Name(s)/ Forename(s)	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing copies of the following documents as proof of identity (please tick the relevant box):

- ☐ Birth Certificate
- ☐ Driving Licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records. please indicate which records these are in the box below.
Please state in which capacity the information is being held (if you know), together with any names or dates (approximate, if necessary) you may have.

Details:

Employment records:
If you are, or have been, employed by the School and are seeking personal information in relation to your employment, please provide the dates of your employment.

Section 2
Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are **NOT** the data subject but an agent appointed on their behalf, you will need to provide evidence of your own identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s) /Forename(s)	
Date of Birth	
Address	
Post Code	
Phone number	
Email address	

I am enclosing copies of the following documents as proof of my identity (please tick the relevant box):

- ☐ Birth Certificate
- ☐ Driving Licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g. parent, carer, legal representative)

I am enclosing a copy of the following document as proof of legal authority to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (please give details):

Section 3
Please describe, in as much detail as possible, the data to which you request access (e.g., time period/categories of data/information relating to a specific case/paper records/electronic records).

I wish to (please tick relevant box):

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we shall take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is sensitive.

Please send your completed form and proof of identity by email to:

admin@woolmore.towerhamlets.sch.uk

Please put the word "confidential" at the start of the subject line.