



# **Data Protection (Privacy) Policy**

**Including:**

**Data Retention Policy**

**Access Request Policy**

**144-148 Park View Road  
Welling  
Greater London  
DA16 1SR**

# Contents

## **Data Protection Policy - p2**

- **Section 1 - Definition - p2**
- **Section 2 - When can the school process personal data - p3**
- **Section 3 - Data Subjects Rights and Requests - p8**
- **Section 4 - Accountability - p10**

## **Data Retention Policy - p15**

## **Subject Access Request Policy - p16**

## **DATA PROTECTION POLICY**

### **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 may 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.

### **SECTION 1 - DEFINITIONS**

#### **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 an opinion about that 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 automatically by reference to the individual or criteria relating to that individual.

#### **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.

#### **Data Subject**

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

## **Data Controller**

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

## **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.

## **Automated Processing**

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.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

## **Data Protection Impact Assessment (DPIA)**

DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

## **Criminal Records Information**

This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures and could include DBS checks.

## **SECTION 2 - WHEN CAN THE SCHOOL PROCESS PERSONAL DATA**

### **Data Protection Principles**

The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the GDPR.

The principles the School must adhere to are: -

- (1) Personal data must be processed lawfully, fairly and in a transparent manner;
- (2) Personal data must be collected only for specified, explicit and legitimate purposes;
- (3) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- (4) Personal data must be accurate and, where necessary, kept up to date;
- (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; and
- (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.

Further details on each of the above principles is set out below.

**Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner**

The School 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: -

- The data subject has given their consent;
- 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;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law; or
- 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 they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- 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 a disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;

- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it 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;
- Where it is necessary for reasons of public interest in the area of public health; or
- The processing is necessary for archiving, statistical or research purposes.

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.

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).

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

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

If explicit consent is required, the School will normally seek another legal basis 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.

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 the data 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 will not collect excessive data and 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 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 to 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 they 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 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: -

- Encryption;
- Pseudonymisation (this is where 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);
- Ensuring authorised access (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles; and
- 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.

Full details on the School's security measures will be set out in the School's Security Policy.

### **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. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the 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;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- 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 to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data 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 of 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 of 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.



### **SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS**

Personal data must be made available to data subjects as set out within this policy and the School's Subject Access Request Policy(below) 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 handle their personal data are set out below: -

- (a) (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time;
- (b) Receive certain information about the School's processing activities;
- (c) Request access to their personal data that we hold;
- (d) Prevent our use of their personal data for marketing purposes;
- (e) 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;
- (f) Restrict processing in specific circumstances;
- (g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) Request a copy of an agreement under which personal data is transferred outside of the EEA;
- (i) Object to decisions based solely on automated processing;
- (j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- (k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- (l) Make a complaint to the supervisory authority; and
- (m) In limited circumstances, 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.

#### **Subject Access Requests**

A Data Subject has the right to be informed by the School of the following: -

- (a) Confirmation that their data is being processed;
- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;

- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of the School's sources of information obtained; and
- (g) 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.
- (h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the Head Teacher who's details can be found on the school website. Full details on how you can make a subject access request are contained within the Subject Access Request Policy which is available below.

### **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: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- 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 details about our security processes; and
- 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; and
- Not to store personal information on local drives.
- Not to download any personal information from the school drive onto personal devices or away from the school environment, without prior consent.

## **SECTION 4 - 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 have taken the following steps to ensure and document GDPR compliance: -

### **Data Protection Officer (DPO)**

Please find below details of the School's Data Protection Officer: -

David Cowell

[david.cowell@alpschools.org](mailto:david.cowell@alpschools.org)

Tel - 0203 1373630

Address - Pierview Academy, 42-46 Harmer Street, Gravesend, Kent, DA12 2AX

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with 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. In particular, you must always contact the DPO in the following circumstances: -

- (a) If you are unsure of the lawful basis being relied on by the School to process personal data;
- (b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- (c) If you need to draft privacy notices or fair processing notices;
- (d) If you are unsure about the retention periods for the personal data being processed but please refer to the School's data retention policy in the first instance;
- (e) If you are unsure about what security measures need to be put in place to protect personal data;
- (f) If there has been a personal data breach please refer to the procedure set out in the School's breach notification policy;
- (g) If you are unsure on what basis to transfer personal data outside the EEA;
- (h) If you need any assistance dealing with any rights invoked by a data subject;
- (i) 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;
- (j) If you plan to undertake any activities involving automated processing or automated decision making;
- (k) If you need help complying with applicable law when carrying out direct marketing activities; or

- (l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

### **Personal Data Breaches**

The GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach.

We will put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where 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. Immediately contact the person or team designated as the key point of contact for personal data breaches (who is The Head Teacher) or your DPO.

The school keeps a log of all data breaches that are reported regardless of their severity.

### **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 which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the School use 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 publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall 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 adopts a privacy by 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 conducts 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: -

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

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

### **Record Keeping**

The School is required to keep full and accurate records of our data processing activities.

These records include: -

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- 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 through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

## **Related Policies**

Staff should refer to the following policies that are related to this data protection policy:

- Data Retention Policy
- Access Request Policy
- Security Policy
- Electronic Information & Communications Systems Policy
- Privacy Notice
- E-safety Policy
- Data Breach Policy
- Policy for Individual Data Rights

These policies are also designed to protect personal data. The first two of these can be found below:

# **Data Retention Policy**

## **The purpose of the retention Policy**

The retention policy lays down the length of time which the record needs to be retained and the action which should be taken when it is of no further administrative use. Members of staff are expected to manage their current record keeping systems using the retention schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems. The retention schedule refers to all information, regardless of the media in which they are stored.

## **What to do with records once they have reached the end of their administrative life**

### **Destruction of records**

Where records have been identified for destruction they should be disposed of in an appropriate way. All records containing personal information, should be shredded before disposal.

### **Transfer of records to the Archives**

Where records have been identified as being worthy of permanent preservation, arrangements should be made to transfer the records to the Archives.

### **Transfer of information to other media**

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

## **School Disposal Schedule:**

The school follows a retention schedule which can be located in a separate document.

# Subject Access Request Policy

## The right of Access

This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act and extended by GDPR . A subject access request can be made in writing or verbally to any part of the School, including by social media. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a subject access request either in writing or is entitled to receive the following::

- confirmation that the School is processing their personal data;;
- a copy of their personal data;
- the purposes of the processing;
- the categories of personal data concerned;
- the recipient or categories of recipient we disclose the personal data to;
- the School's retention period for storing the personal data or, where this is not possible, the criteria for determining how long the school will store it;
- confirmation of the right to request rectification, erasure or restriction or to object to such processing;
- confirmation of the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual
- The existence of automated decision-making (including profiling); and
- the safeguards that the School provides if personal data is transferred to a third country or international organisation.

## Automated Decisions

An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision to grant or deny credit, or an assessment of performance at work (except where this information is a trade secret). Other rights relating to these types of decisions are dealt with in more detail in [Automated decision taking](#).

## Fee

The School may charge reasonable fee for complying the a subject access request:

- where the request is manifestly unfounded or excessive;or
- if the individual requests further copies of their data following a request.

## Time limit for responding to a Subject Access Request

ALP School will respond to a subject access request without undue delay and in any event within one calendar month of receiving it. The time limit is calculated from the day after the request is received until the corresponding date in the next month.

If the School is unable to identify the individual making the Subject Access from the initial request, the time limit will not start to run until the School has received additional information from which they are able to identify the individual.



If the subject access request is complex or if a number of requests are made by the same individual, the School may extend the time to respond by a further two months. If the School extends the time limit it will let the individual know within one month of their request and will explain why the extension is necessary.

### **Responding to data requests about a child**

Even if a child is too young to understand the implications of a subject access request it is still the right of the child. In the case of very young children the rights are likely to be exercised by those with parental responsibility (Further information about Parental Responsibility can be found here:

<https://childlawadvice.org.uk/information-pages/parental-responsibility/>.

Before responding to a subject access request about a child, the School will consider whether the child is mature enough to understand their rights. If the School is confident that the child understands their right, the response will be sent directly to the child. The School will allow the parent to act on behalf of the child if the child has given his or her consent or if it is clearly in the best interests of the child.

### **Borderline cases**

If the School considers that a child's understanding of the implications of a subject access request are borderline the following will be taken into account:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- 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;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

### **Exemptions**

The School may refuse to comply with a Subject Access Request if it is manifestly unfounded or excessive taking into account whether the request is repetitive in nature.

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a Subject Access Request. Guidance on such Exemptions will be taken from the ICO

### **Providing the Individual with Reasons**

If the School refuses to comply with a Subject Access Request, charges a Fee or requires further information to enable it to identify an individual it will inform the individual about:

- the reasons that the school is not taking action;
- their rights to make a complaint to the ICO or another supervisory body; and
- their ability to seek to enforce this right through a judicial remedy.

In the event of an access request the school will take the following steps with guidance from the DPO:

1. Determine if the request is a Subject Access Request - (Any written request by an individual asking for their personal information is a subject access request). Determine if the school has enough information to be sure of the requestor's identity. If the answer is no, the school will ask for any evidence that is necessary to confirm who they are.. This will be done promptly.
2. The school will decide if a fee is required.
3. The school will see if we have the information the requester wants. If the school does not, the requester will be told.
4. A decision will be made on whether any of the information needs to be changed before a response is sent. The school will not make changes to records as a result of receiving the request, even if the information is inaccurate or embarrassing.
5. The school will check to see if the data requested includes information about other people. If it does the school does not have to supply the information unless the other people mentioned have given their consent for the disclosure, or it is reasonable to supply the information without their consent. If the school decides not to disclose the other people's information, we will still disclose as much information as possible by redacting the references to them.
6. If the information the school is supplying includes any complex terms and/or codes, these will be explained.
7. The response will be prepared in a permanent form unless the individual agrees otherwise, or doing so is impossible or would involve disproportionate effort.
8. If an individual makes a request electronically, the school will use all reasonable endeavours to provide the information requested in a commonly used electronic format unless the individual requests otherwise.