

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 1 of 16

Table of Contents

Aims.....	1
Statutory Requirements	2
UK General Data Protection Regulation (GDPR)	2
General Data Protection Principles	2
Data Protection Controller	6
Roles and Responsibilities	6
Data Protection Officer	7
What is Personal Information?	9
Definitions:	9
School Site Procedures & Data Security	10
Personal Data Breach Reporting.....	10
Data Security and Storage of Records	122
Providing Information to Third Parties	12
Subject Access Requests	13
Children and subject access requests.....	14
Responding to subject access requests	15
Links with other policies	16
Complaints.....	17
Approval/Amendment.....	17
Questions.....	17

Aims

Woodford County High School is obliged to collect and use personal information about current, past and prospective employees, governors, students, parents, guardians, suppliers and other third parties who come into contact with the school. This information is gathered in order to enable the school to provide education and other associated functions.

The purpose of this policy is to ensure that personal information is dealt with correctly and securely and in accordance with the UK General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026
	Last modified: 3 rd June 2026
	Document no SP 03.01.006
	Replaces Version: 17 th January 2024
	Approved: Finance & General Business Committee Page 2 of 16

Woodford County High School will take all reasonable steps to process personal information in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. In this Policy, any reference to students includes current, past or prospective students.

This policy applies to all users who handle information belonging to the school regardless of their work location i.e. on the school site, at home, remote or mobile working and applies to all personal data collected, handled, stored, transmitted or shared. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities as detailed in this Policy.

Statutory Requirements

UK General Data Protection ACT 2018

This policy meets the requirements of, but not limited to the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#). [The Freedom of Information Act 2000](#) , [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#) and [The School Standards and Framework Act 1998](#)

It also meets the requirements of:

- The [Protection of Freedoms Act 2012](#) when referring to the use of biometric data.
- The ICO's [code of practice](#) for the use of surveillance cameras and personal information.
- In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#) (As amended in 2016), which gives parents the right of access to their child's educational record.

UK General Data Protection Regulation (GDPR)

UK General Data Protection Regulation replaces the previous Data Protection Directives that were in place. It was approved by the EU Parliament in 2016 and comes into effect on 25th May 2018.

GDPR states that personal data should be 'processed fairly & lawfully' and 'collected for specified, explicit and legitimate purposes' and that an individual's data should not be processed without their knowledge but only with their 'explicit' consent. GDPR covers personal data relating to individuals. Woodford County High School is committed to protecting the rights and freedoms of individuals with respect to the processing of children's, parents', visitors' and staff personal data.

The General Data Protection Regulation gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly

General 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 UK GDPR. The principles the school must adhere to are set out below.

 Woodford County High School for Girls	Effective Date: 9 th June 2026
	Last modified: 3 rd June 2026
	Document no SP 03.01.006
	Replaces Version: 17 th January 2024
	Approved: Finance & General Business Committee Page 3 of 16

SCHOOL POLICY

Data Protection

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 data as set out in the UK 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;
- 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 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;

SCHOOL POLICY

Data Protection

Effective Date:	9 th June 2026
Last modified:	3 rd June 2026
Document no	SP 03.01.006
Replaces Version:	17 th January 2024
Approved: Finance & General Business Committee	Page 4 of 16

- 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;
- 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 UK 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 UK 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).

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 5 of 16

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.

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.

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026
	Last modified: 3 rd June 2026
	Document no SP 03.01.006
	Replaces Version: 17 th January 2024
	Approved: Finance & General Business Committee Page 6 of 16

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 on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the process for which it is processed.

The School follow 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.

Data Protection Controller

All schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. This information is then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all students and parents; this summarises the information held on students, why it is held and the other parties to whom it may be passed on.

Roles and Responsibilities

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Record of Processing Activities (ROPA)

The school maintains a comprehensive Record of Processing Activities (ROPA) in accordance with Article 30 of the UK General Data Protection Regulation. This record documents all processing activities

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026
	Last modified: 3 rd June 2026
	Document no SP 03.01.006
	Replaces Version: 17 th January 2024
	Approved: Finance & General Business Committee Page 7 of 16

involving personal data and includes:

- The purpose of the processing
- Categories of data subjects and personal data
- The lawful basis for processing
- Categories of recipients of personal data
- Details of transfers to third countries (if applicable)
- Retention periods for each category of data
- A general description of technical and organisational security measures

The ROPA is reviewed regularly and updated to reflect any changes in processing activities. Responsibility for maintaining the ROPA sits with the School Business Manager, with oversight from the Data Protection Officer (DPO).

Governing Board

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

Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and for providing advice and guidelines where applicable. The school's Data Protection Officer is

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

Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK 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: -

- If you are unsure of the lawful basis being relied on by the school to process personal data;
- If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- If you need to draft privacy notices or fair processing notices;
- If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Retention Policy in the first instance];

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 8 of 16

- (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 [and would refer you to the procedure set out in the School's Data Breach 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;
- (l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

Data Protection Impact Assessments (DPIAs)

The school will carry out a Data Protection Impact Assessment (DPIA) for any processing activity that is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA will be required in situations including, but not limited to:

- The introduction of new technologies or systems involving personal data
- Large-scale processing of special category data
- Systematic monitoring of individuals (e.g. CCTV or tracking systems)
- Any significant change to existing processing activities

The DPIA process will:

- Assess the necessity and proportionality of the processing
- Identify and evaluate risks to individuals
- Set out measures to mitigate those risks

The Data Protection Officer must be consulted as part of the DPIA process, and no high-risk processing will commence until appropriate safeguards have been identified and implemented.

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
 - If they have any concerns that this policy is not being followed
 - If they are unsure whether or not they have a lawful basis to use personal data in a

SCHOOL POLICY

Data Protection

Effective Date:	9 th June 2026
Last modified:	3 rd June 2026
Document no	SP 03.01.006
Replaces Version:	17 th January 2024
Approved: Finance & General Business Committee	Page 9 of 16

- particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals or if they need help with any contracts or sharing personal data with third parties

Staff must only process personal data where it is necessary in order to do their job

When staff no longer need the personal data they hold, they must ensure it is deleted/shredded or pseudonymous. This will be done in accordance with the Records Management Society's Retention Guidelines for Schools.

What is Personal Information?

Personal information is information that the school collects about staff, pupils and parents. This includes information such as name, date of birth, National Insurance Number, address as well as exam results, medical details, nationality and behaviour records. The school may also record religion and ethnicity.

Definitions:

Personal Data: personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by:

- reference to an identifier such as a name,
- identification number,
- location data,
- an online identifier
- It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity

Special categories of personal data: Personal data which is more sensitive and so needs more protection, including information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 10 of 16

- Health – physical or mental
- Sex life or sexual orientation

Processing: Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data Subject: The identified or identifiable individual whose personal data is held or processed.

Data Controller: A person or organisation that determines the purposes and the means of processing of personal data.

Data Processor: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller

Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

School Site Procedures & Data Security

GDPR requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if said third party agrees to comply with those procedures and policies, or puts in place adequate measures themselves. Woodford County High School will take all reasonable steps to ensure that members of staff will only have access to personal data relating to students, their parents or guardians where it is necessary for them to do so. Woodford County High School is committed to maintaining the above principles at all times.

Personal Data Breach Reporting

All staff must report any actual or suspected personal data breach immediately to the School Business Manager and Data Protection Officer.

A personal data breach includes any incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Where a breach is likely to result in a risk to the rights and freedoms of individuals, the school will notify the Information Commissioner's Office (ICO) without undue delay and, where feasible, within **72 hours** of becoming aware of the breach.

 SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026
	Last modified: 3 rd June 2026
	Document no SP 03.01.006
	Replaces Version: 17 th January 2024
	Approved: Finance & General Business Committee Page 11 of 16

Where the breach is likely to result in a high risk to individuals, affected data subjects will also be informed without undue delay.

All breaches will be recorded internally, including those not reported to the ICO, in accordance with accountability requirements.

Therefore, the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary or legally required
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded (paper files or on our computer system)
- Share personal information with others only when it is necessary and legally appropriate to do so
- Set out clear procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests in the UK General Data protection regulation
- Train our staff so that they are aware of and understand our policies and procedures

All staff will be made aware of this policy and their duties under the UK General Data Protection Regulation and the school will ensure that all personal information is held securely and is not accessible to unauthorised persons and will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data.

Security procedures include:

1. The school has electronic gates installed
2. We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.
3. The school operates a key fob entry system
4. Equipment - data users should ensure that individual monitors do not show confidential information to passers-by and that they log off / or lock their PC when it is left unattended.

 SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 12 of 16

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular

1. Secure lockable desks and cupboards - desks and cupboards are kept locked if they hold confidential information of any kind (personal information is always considered confidential).
2. Methods of disposal - paper documents are shredded or placed in dedicated confidential document bins located around the site, data storage devices are physically destroyed when they are no longer required
3. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
4. Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are prompted to change their passwords every 90 days.
5. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
6. Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our ICT Acceptable Use Policy).
7. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Providing Information to Third Parties

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us

In particular they should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;
- Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;
- Refer to the head teacher for assistance in difficult situations;
- Where providing information to a third party, do so in accordance with the data protection principles.

SCHOOL POLICY

Data Protection

Effective Date:	9 th June 2026
Last modified:	3 rd June 2026
Document no	SP 03.01.006
Replaces Version:	17 th January 2024
Approved: Finance & General Business Committee	Page 13 of 16

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

All data subject access requests should be immediately directed to the School Business Manager who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the school must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). Neither are they entitled to information simply because they may be interested in it. So, it is important to establish whether the information requested falls within the definition of personal data. In most cases, it will be obvious whether the information being requested is personal data, but we have produced separate guidance to help you decide in cases where it is unclear: *Determining what is personal data (pdf)*. Please also see the key definitions.

Subject access provides a right to see the information contained in personal data, rather than a right to see the documents that include that information.

This includes:

- confirmation that you are processing their personal data
 - Access to a copy of the data
 - The purposes of the data processing
 - The categories of personal data concerned
 - Who the data has been, or will be, shared with
 - How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
 - They can request rectification, erasure or restriction or to object to such processing;
 - The source of the data, if not the individual
 - Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:
- Name of individual
 - Correspondence address
 - Contact number and email address
 - Details of the information requested
- If staff receive a subject access request they must immediately forward it to the SRO

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 14 of 16

Children and subject access requests

The school need 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.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

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.

It shall be assessed if 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, it should be taken into account, among other things:

- 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.

•

Generally, a person aged 12 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 12 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 require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

 SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026
	Last modified: 3 rd June 2026
	Document no SP 03.01.006
	Replaces Version: 17 th January 2024
	Approved: Finance & General Business Committee Page 15 of 16

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.

Responding to subject access requests

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

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO

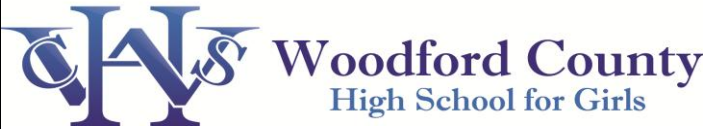
Governance, Monitoring and Assurance

The school is committed to maintaining a high standard of data protection compliance through effective governance, monitoring and continuous improvement.

Data Protection Governance

The Governing Board has overall responsibility for ensuring that the school meets its data protection obligations. Regular updates on data protection compliance, risks and incidents will be provided to Governors as part of the school's governance and assurance framework.

The Headteacher and School Business Manager are responsible for the day-to-day implementation of this policy, with oversight and advisory support provided by the Data Protection Officer (DPO).

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 16 of 16

Training and Awareness

The school will ensure that all staff receive appropriate data protection training, including:

- Mandatory data protection training as part of staff induction
- Regular refresher training (at least annually)
- Additional targeted training where roles involve higher-risk data processing

Training records will be maintained to demonstrate compliance with accountability requirements.

Privacy Notices

The school will maintain clear and up-to-date privacy notices for all key groups, including pupils, parents, staff and visitors.

These notices will:

- Explain how personal data is collected, used and shared
- Be easily accessible, including via the school website
- Be reviewed regularly and updated where processing activities change

Monitoring and Audit

The school will implement a programme of monitoring and review to ensure continued compliance with data protection legislation. This will include:

- Periodic internal data protection audits
- Reviews of data protection practices and procedures
- Monitoring of compliance with this policy and associated procedures

Findings from audits and reviews will be reported to senior leadership and, where appropriate, to the Governing Board.

Continuous Improvement

The school will take steps to continuously improve data protection practices by:

- Reviewing policies and procedures at least annually
- Responding to guidance from the Information Commissioner's Office (ICO)
- Learning from data breaches, incidents or near misses
- Updating training, processes and controls where necessary

Links with other policies

This data protection policy is linked to the following school policies:

SP04.04 Freedom of Information Publication Scheme
SP03.04 ICT Acceptable Use Policy Staff/Student/parents)

 Woodford County High School for Girls SCHOOL POLICY Data Protection	Effective Date: 9 th June 2026	
	Last modified: 3 rd June 2026	
	Document no SP 03.01.006	
	Replaces Version: 17 th January 2024	
	Approved: Finance & General Business Committee	Page 17 of 16

SP04.01 Safeguarding and Child Protection Policy

SP03.07 ICT eSafety Policy

SP02.11 Staff Code of Conduct

SP03.08 Data Retention Policy

SP03.09 Data Breach Policy

Complaints

Complaints will be dealt with in accordance with the school's Complaints Policy (SP05.07). Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Further advice and information is available from the Information Commissioner's Office:

http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx

Approval/Amendment

This policy is approved by the Governing Board of Woodford County High School. Any Amendments to this Policy will be updated as necessary to reflect best practice or amendments made to the UK General Data Protection regulations and will require approval by the Governing Board of Woodford County High School.

Questions

If you have any questions about this present statement of policy, please contact the School Business Manager at Woodford County High School, High Road, Woodford Green, Essex, IG8 9LA, who will also act as the contact point for any subject access requests.

Further advice and information, including a full list of exemptions, is available from the Information Commission, www.informationcommissioner.gov.uk