WANSTEAD HIGH SCHOOL

Data Protection, Breach & Retention Policy

(including SAR procedure)

Person Responsible	Ms S Williams
Review Frequency	Annually
Last Reviewed	Autumn Term 2025
Next Review Date	Autumn Term 2026
Committee	Resources
Ratified by Full Governing Body on	26 January 2026
This policy is communicated by the following means	Website

Version History Log

Version	Description of Change	Date of Judicium Policy Release	Date of Policy Change
Data Protection Policy:			
1	Initial Issue	6.05.2018	
2	Addition of SAR appendix. Updated with DPO details. Added details on school closure periods.		
3	Updated to reflect UK GDPR, including details for international transfers outside of UK.		
4	Merged SAR Policy entirely into SAR Appendix.		
5	Removal of duplicated third part	30.12.2021	
6	Formatting changes	02.08.2022	
7	Correction of Article 9 conditions for processing Minor grammar and spelling edits Update Judicium contact details	05.03.2024	
8	Updated 'Requesting Clarification of the Request'. Added page numbers.	26.03.2024	
Data Breach Policy:			
1	Initial Issue	06.05.18	
2	Updated with DPO details - updated to CS.		
3	Updated references to UK GDPR.		
4	Added cyber security policy reference, training section and acknowledgement of reading the policy wording	19.08.21	
5	Created a New Data Breach Policy for Wanstead High School using a Judicium template.	01.05.2022	
6	Formatting amendments	03.08.2022	
Data Protection, Breach and Retention Policy:			
1	Combined Data Protection Policy (Version 8) and Data Breach Policy (Version 6) and added Data Retention Policy. *(Data Protection Policy and Data Breach Policy retired).*		September 2024

Contents

1. Introduction

Wanstead High School is committed to protecting and respecting individual privacy. The specific purpose of this Policy is to ensure that the school complies with UK data protection laws regulating the use of information concerning living individuals. In particular, the school is obliged to comply with **UK GDPR**.

UK 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 UK GDPR. This Policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties, including where a data breach occurs.

This Policy comprises three main parts:

- **Section A**: Data Protection
- **Section B**: Data Breach
- **Section C**: Data Retention

It also includes the following Appendices:

- Appendix 1 – Data Retention Schedule
- Appendix 2 - Subject Access Request (**SAR**) Procedure

This Policy applies to all **Staff** of WHS, which includes teachers, associate staff, governors and all who work on the school site, including volunteers, where their work brings them into contact with Personal Data (defined below). All members of Staff are required to familiarise themselves with, and comply with, this Policy. This Policy does not form part of any Staff member's contract of employment and is not intended to have contractual effect. It does, however, reflect the school's current practice, the requirements of current legislation and best practice and guidance, and failure to comply with it may result in disciplinary action.

This Policy should be read together with the school's E-Safety Policy (which incorporates the Social Media Policy and the ICT Acceptable Use Policy).

2. Definitions

Automated Processing	Any form of automated processing (defined below) of Personal Data (defined below) 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 (without human intervention) which produces legal effects or significantly affects an individual. Automated decision-making is prohibited except in exceptional circumstances.
Criminal Record Information	Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
Data Controller Data Processor	UK GDPR draws a distinction between a 'controller' and a 'processor' in order to recognise that not all organisations involved in the processing of Personal Data have the same degree of responsibility: • A 'Controller' is a person or entity which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. • A 'Processor' is a person or entity which processes Personal Data on behalf of the Controller. For the purposes of this Policy, **WHS is a Data Controller.**
Data Protection Officer (DPO)	The DPO assists the school in monitoring internal compliance, informing and advising on its data protection obligations, providing advice regarding Data Protection Impact Assessments (DPIAs) and acting as a contact point for data subjects and the Information Commissioner. WHS has appointed Judicium Consulting Limited as its DPO: Data Protection Officer: Judicium Consulting Limited Address: 5th Floor, 98 Theobalds Road, London WC1X 8WB Email: dataservices@judicium.com Web: www.judiciumeducation.co.uk Telephone: 0345 548 7000 (Option 1, then 1)
Data Subject	An individual whose Personal Data (defined below) is processed (defined below) is known as the Data Subject.
Data Protection Impact Assessment (DPIA)	A DPIA is a tool used to identify risks in data processing activities with a view to reducing them.

Information Commissioner's Office (ICO)	The UK's independent regulator for data protection and information rights.
Legitimate Interests condition	This condition is met where Personal Data is processed and: • There is a legitimate interest behind the processing (the "purpose"); • The processing is "necessary" for that purpose (i.e. the purpose(s) could not reasonably be achieved without the relevant processing); and • The legitimate interest is not overridden by the Data Subject's interests, rights of freedoms (i.e. either the processing does not prejudice the privacy of the affected Data Subject or, if there is some prejudice, it is sufficiently trivial or minor that it does not override the need to pursue those legitimate interests.)
Personal Data	Personal Data is a very broad term – it means information that: • relates to a living individual who can be identified or is identifiable (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access; and • is held either (i) on computer or in other electronic or automatically processable form; or (ii) in a paper filing system arranged to be accessible according to specified criteria. This includes Special Category Data (defined below) 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 (e.g. a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Information does not have to be particularly personal or private to constitute Personal Data. Information qualifies as Personal Data when an individual can be identified from the information, and so simply the name of a person (a Data Subject) or their contact details might constitute Personal Data.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data or Special Category Data transmitted, stored or otherwise processed.
Privacy Statement	Document available on the school website which sets out the information that the school must provide to Data Subjects before any processing (defined below) of their Personal Data begins.
Processing	Processing is a very broad term – it means any activity that involves the use of Personal Data (defined above). This includes obtaining/collecting, recording or storing/holding that data – but also carrying out any operation or set of operations on that data such as analysing, using, disclosing, amending, archiving, retrieving, deleting, erasing or destroying it.

	Processing also includes transmitting or transferring personal data to third parties. "Process", "Processed" and "Processable" should be read accordingly.
Processing System	This Policy refers to an information technology system or other arrangement involving the processing of Personal Data as a processing system.
Special Category Data	Special Category Data is a subset of Personal 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 opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data. For the purposes of this Policy, Special Category Data includes data relating to an individual's Criminal Record Information.
Staff	For the purpose of this policy, Staff includes teachers, associate staff, governors and all who work on the school site, including volunteers.
Subject Access Request (SAR)	A request made by or on behalf of an individual for the information which they are entitled to ask for under Article 15 UK GDPR. The right of access gives someone the right to obtain a copy of their personal information from an organisation, including where the information came from, what it is being used for, and who it is being shared with. UK GDPR does not set out formal requirements for a valid request, so an individual can make a SAR verbally or in writing.
UK GDPR	UK GDPR means the UK data protection laws which the school is required to comply with, and specifically the requirements and restrictions of the General Data Protection Regulation (EU) 2016/679 as it forms part of UK law by virtue of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

3. Data Protection Officer

The Data Protection Officer (**DPO**) is responsible for overseeing this Policy and developing data-related policies and guidelines. WHS has appointed Judicium Consulting Limited to act as its DPO:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (Option 1, then 1)

Please contact the DPO with any questions about the operation of this 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, having referred to the Consent guidance in Part A of this Policy, you need to rely on consent as a fair reason for processing;
- If you need to draft privacy notices or fair processing notices;
- If, having referred to Part C: Data Retention of this Policy, you are unsure about the retention periods for the Personal Data being processed;
- If you are unsure about what security measures need to be put in place to protect Personal Data;
- If, having referred to Part B: Data Breach of this Policy, there has been a Personal Data Breach;
- If you are unsure on what basis to transfer Personal Data outside the EEA;
- If you need any assistance dealing with any rights invoked by a Data Subject;
- 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;
- If you plan to undertake any activities involving automated processing or automated decision making;
- If you need help complying with applicable law when carrying out direct marketing activities; and
- If you need help with any contracts or other areas in relation to sharing Personal Data with third parties.

4. Accountability

The school will ensure compliance with data protection principles by implementing appropriate technical and organisational measures.

The school has taken the following steps to ensure accountability for UK GDPR compliance:

Privacy by Design

The school adopts a privacy by design approach to data protection to ensure that it adheres to data compliance requirements 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 UK 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; and

- for large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

The school's 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.

Training

The school will ensure that Staff receive training to enable them to comply with this Policy, meet their data protection obligations and be aware of the need to immediately report potential or known Personal Data Breaches in accordance with this Policy.

Monitoring and audit

The school will monitor the effectiveness of this Policy and submit it for annual (or more frequently where a breach incident indicates review is required) review and approval by the Governing Body. The school, through its DPO, regularly test its data systems and processes in order to assess compliance. This is done through data audits which take place annually in order to review use of personal data.

PART A: DATA PROTECTION

Headline guidance for staff

You 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 you to help the school meet its 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 (e.g. by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction);
- Not 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;
- Not store personal information on local drives; and
- Not transfer Personal Data to another country outside of the EEA, noting that a transfer of data to another country can occur when you transmit, send, view or access that data (eg. reading school emails that contain Personal Data) in that country.

Please also refer to the school's **E-Safety Policy** (incorporating the Social Media Policy and ICT Acceptable Use Policy for further details on the school's expectations of staff and others when using ICT.

If you know or suspect that there has been a breach of Personal Data, whether by you or another, and whether intentional or accidental, please refer to Part B (Data Breach) of this Policy.

Further information on the above is set out in the rest of this Policy, which you must familiarise yourself with, and comply with, at all times.

5. What Personal Data does the School Process?

"**Personal Data**" is a very broad term. It can be factual (e.g. a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Information does not have to be particularly personal or private to constitute Personal Data. Information qualifies as Personal Data when an individual can be identified from the information, and so simply the name of a person (a Data Subject) or their contact details might constitute Personal Data.

Some examples of Personal Data which the school processes are:

- Names and dates of birth of pupils and staff and others.

- Addresses of, parents, pupils and staff.
- Exam results, school assessments and grades.
- Financial records, such as Staff tax information and bank details.
- Staff performance reviews.

Some examples of Special Category Data which the school processes are:

- Information about pupils' racial or ethnic origin.
- Information about staff disabilities.
- Medical records, including GP names and medical conditions.
- Safeguarding information, including data related to special educational needs and disabilities (SEND) assessments.

"**Processing**" is also a very broad term – it means collecting, storing, analysing, using, disclosing, archiving, deleting or doing absolutely anything else with Personal Data (and "Process", "Processed" and "Processable" should be read accordingly). This Policy refers to an information technology system or other arrangement involving the processing of Personal Data as a **Processing System**. The school uses a number of processing systems, including SIMS, a student information system and school management information system.

This Policy uses the term "**Data Subject**" to describe those whose Personal Data the school processes.

6. When can the school process Personal Data?

Key principles of data protection

The school can process Personal Data if it adheres to the key principles in UK GDPR. All staff are required to be aware of and comply with these principles when processing Personal Data on behalf of the school.

The key principles can be summarised as follows (further detail on each is set out below):

- Lawfulness, fairness and transparency: The school must process Personal Data lawfully, fairly and in a transparent manner.
- Purpose limitation: The school must collect Personal Data only for specified, explicit and legitimate purposes (and not process it in a manner that is incompatible with those purposes).
- Data minimisation: The school must only collect Personal Data which is adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- Accuracy: The school must keep accurate Personal Data and, where necessary, keep it up to date (and erase or rectify any inaccuracies without delay).
- Storage limitation: The school must keep Personal Data for no longer than is necessary for the purposes for which it is processed.
- Integrity and confidentiality: The school must process Personal Data in a manner that ensures appropriate security of the data.

PRINCIPLE 1: Lawfulness, fairness and transparency

The school must process Personal Data lawfully, fairly and in a transparent manner.

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 (ie. that there is no other reasonable way to achieve that purpose).

Provision of information to Data Subjects

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 UK GDPR. This includes the identity of the Data Protection Officer (DPO), the school's contact details, how and why we will use, process, disclose, protect and retain Personal Data. 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. These are tailored to suit the data subject and set out information about how the school use their Personal Data. *The school's* ***Privacy Statement*** *can be found on its website.*

The school will establish and follow procedures to ensure that, unless it can rely on the lawful bases for processing set out below, Data Subjects who provide Personal Data to the school are provided with the information in the privacy notices, if they do not already have it, before any processing of their Personal Data begins.

When personal data is collected indirectly (eg. from a third party or a publicly available source), where appropriate, 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 UK 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 UK GDPR.

However, the school does not need to provide Data Subjects with the information in the privacy notices in the following circumstances:

- if the relevant Personal Data is not obtained by the school directly from the Data Subject but from a third party, and to contact and inform the Data Subject would be impossible, or would require effort disproportionate to the value to the Data Subject of being informed;
- if the school is processing the relevant Personal Data in order to investigate an alleged or actual crime, regulatory breach or disciplinary issue, and to provide the information would prejudice the investigation in accordance with applicable law; or
- otherwise, if the DPO has concluded in writing that the UK GDPR and other applicable laws do not require the information to be provided.

Lawful basis for Processing

The school will not process Personal Data unless it can be done on one of the following lawful bases:

- Legitimate Interests. This condition has three key elements or tests:

1. *Purpose test* – is there a "legitimate interest" behind the processing?

- A wide range of interests may be legitimate interests. It could be the school's legitimate interests in the Processing or it could include the legitimate interests of any third party.
- The legitimate interests of the public in general may also play a part when deciding whether the legitimate interests in the processing override the Data Subject's interests and rights. If the processing has a wider public interest for society at large, then this may add weight to the school's interests when balancing these against those of the Data Subject.

2. *Necessity test* – is the processing necessary for that purpose?

    - ie. the purpose(s) could not reasonably be achieved without the relevant processing.

3. *Balancing test* – is the legitimate interest overridden by the Data Subject's interests, rights or freedoms?

    - A risk to individuals' rights and freedoms is about the potential for any type of impact and includes physical, financial or any other impact (e.g. inability to exercise rights (including data protection rights); loss of control over the use of Personal Data; or any social or economic disadvantage). In essence, this is a light-touch risk assessment to check that any risks to individuals' interests are proportionate – so either the processing does not prejudice the affected Data Subject or, if there is some prejudice, it is sufficiently trivial or minor that it does not override the need to pursue those legitimate interests.
    - If the data belongs to children, then the school needs to be particularly careful to ensure their interests and rights are protected.

    - Consent: The Data Subject has given clear consent for the school to process their Personal Data for a specific purpose*:*

        - Consent must be freely given, specific, informed and be an unambiguous indication that the Data Subject wishes to agree to the processing of Personal Data relating to them.
        - A Data Subject can consent to processing of their *non*-Special Category Data if they indicate agreement clearly either by a statement or *positive* action to the processing.
        - This means that affirmative action is required - 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.
        - The school will keep records of consents obtained in order to demonstrate compliance with consent requirements under UK GDPR.

    - Contract: The processing is necessary for a contract with the Data Subject, or because they have asked you to take specific steps before entering into a contract.

    - Legal obligation: The processing is necessary for the school to comply with the law.[1]

[1] The legal obligation must be an obligation arising under the law of the United Kingdom, and a *contractual* obligation is not a legal obligation for these purposes.

- Vital interests: The processing is necessary to protect someone's life.

- Public task: The processing is necessary for the school to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.

Lawful basis for Processing Special Category Data

Special Category Data is subject to different rules - the school may only process Special Category Data on one of the following lawful bases:

- Explicit consent: The Data Subject has given their "explicit" consent:

    - This mean that a very clear and specific statement of consent to be relied upon is required.
    - The school will normally seek another legal basis to process Special Category Data. However, if explicit consent is required, the Data Subject will be provided with full information in order to provide that consent.

- Employment, social security and social protection law: 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.

- Vital interests: To protect the Data Subject's vital interests.

- Made public by the Data Subject: The data has been made public by the Data Subject.

- Legal claims and judicial acts: The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

- Substantial public interest: To perform a task in the substantial public interest or in order to carry out official functions as authorised by law.

- Health or social care: The processing 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.

- Public health: The processing is necessary for reasons of public interest in the area of public health.

- Archiving, research and statistics: The processing is necessary for archiving, statistical or research purposes.

PRINCIPLE 2: Purpose limitation

The school must collect Personal Data only for specified, explicit and legitimate purposes (and not process it in a manner that is incompatible with those purposes).

The school will only process Personal Data fairly and for the specified purposes of carrying out its operations in order to fulfil its functions and obligations as a co-educational comprehensive secondary school.

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: Data Minimisation

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 will ensure any Personal Data collected is adequate and relevant for the intended purposes.

PRINCIPLE 4: Accuracy

The school must keep accurate Personal Data and, where necessary, keep it up to date (and erase or rectify any inaccuracies without delay).

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 have the right to request rectification to incomplete or inaccurate data held by the school.

PRINCIPLE 5: Storage limitation

The school must keep Personal Data in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which it is processed.

The school will ensure that it adheres to relevant timeframes for retaining data, which will include taking into account the need to satisfy legal, accounting and other reporting requirements.

When Personal Data is no longer needed for specified purposes, the school will take reasonable steps to destroy or erase that data from its systems.

The school will also ensure that Data Subjects are informed of the period for which data is stored and how that period is determined in its Privacy Statement (a copy of which is on the school's website).

The school's Data Retention Policy at Part C of this Policy sets out further details on how the school retains and removes data.

PRINCIPLE 6: Integrity and confidentiality

The school must process Personal Data in a manner that ensures appropriate security of the data.

In order to ensure the protection of Personal Data being processed, the school will develop, implement and maintain reasonable safeguards 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 follows procedures and technologies to ensure security of data and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing Personal Data.

*The school's ICT security measures and responsibilities are summarised in the school's **E-Safety Policy**.*

Sharing Personal Data

The school will generally not share Personal Data with third parties unless suitable safeguards and contractual arrangements have been put in place. The following points will be considered:

- whether the third party has a need to know the information for the purposes of providing the contracted services;
- whether sharing the Personal Data complies with the privacy notice that has been provided to the Data Subject;
- whether the Data Subject's consent has been obtained;
- whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- whether the transfer complies with any applicable cross border transfer restrictions; and
- whether a fully executed written contract that contains UK GDPR compliant 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 (e.g. the Local Authority, Ofsted or the Department of Health). These authorities have their own policies and procedures relating to the protection of any Personal Data that they receive or collect.

The intention to share Personal Data outside of the school shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data Outside the European Economic Area (EEA)

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

The school will not transfer data to another country outside of the EEA without appropriate safeguards in place and unless doing so is in compliance with the UK 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 (e.g. reading school emails that contain Personal Data) in that particular country.

The school may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of data protection legislation, or alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, standard contractual clauses or compliance with an approved code of conduct.

4. Data Subject rights and requests

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 school's SAR Procedure is at Appendix 2 to this Policy**, and provides guidance for:*

- *Staff on how data SARs should be handled; and*
- *individuals on how to most effectively make a SAR to the school.*

Failure to comply with the right of access under UK GDPR puts both staff and the school at potentially significant risk and so the school takes compliance with its SARs Procedure very seriously.

Data Subjects also have a number of other rights in relation to their Personal Data, including to:

a) (Where consent is relied upon as a condition of processing) withdraw consent to processing at any time;
b) receive certain information about the school's processing activities;
c) prevent our use of their Personal Data for marketing purposes;
d) ask us to erase Personal Data if: it is no longer necessary in relation to the purposes for which it was collected or processed;
e) ask us 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 (the ICO); 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.

Data Subjects also have the right to the following:

n) to confirmation from the school that their Personal Data is being processed;
o) a description of the Personal Data that is being processed;
p) the purpose for which the Personal Data is being processed;
q) the recipients/class of recipients to whom the Personal Data is or may be disclosed;

r) details of the source(s) from which the school has obtained the Personal Data;
s) to be provided with a copy of any Personal Data that the school holds about them, with certain related information;
t) to require the school, without undue delay, to update or correct any inaccurate Personal Data, or complete any incomplete Personal Data, concerning them;
u) to require the school to stop processing their Personal Data for direct marketing purposes;
v) 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 them, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, data concerning performance at work, creditworthiness, reliability and conduct;
w) to object to the processing of their Personal Data more generally; and

Data Subjects may also have the right, in certain circumstances:

x) to require the school, without undue delay, to delete their Personal Data;
y) to "restrict" the school's processing of their Personal Data, so that it can only continue subject to very tight restrictions; and
z) to require Personal Data which they have provided to the school, and which is processed based on their Consent or the performance of a contract with them, to be "ported" to them or a replacement service provider.

5. Direct marketing

The school is subject to certain rules and privacy laws when marketing. This includes that a Data Subject's prior consent will be required for electronic direct marketing (eg. 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.

6. Obligations of Data Processors

A Data Processor is a person or entity which processes Personal Data on behalf of the Controller (the school).

This policy is to be provided to Data Processors who process Personal Data on behalf of the school, and they shall be obliged to notify the Data Protection Lead as soon as possible if they become aware of a Data Breach. Failure to do so may breach the processing agreement between the school and the Data Processor, or allow the school to terminate that agreement without notice.

7. Automated Processing and automated decision making

Automated decision making is generally prohibited when a decision has a legal or similar significant effect on an individual unless:

a) the Data Subject has given explicit consent;
b) the processing is authorised by law; or
c) the processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest (e.g. fraud prevention).

If a decision is to be based solely on automated processing, then data subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

The school does not generally carry out automated decision making, but may do so in the future (e.g. by using online algorithms or time management performance systems which are not monitored or evaluated by individuals – i.e. that the results are generated solely by automation). If it does intend to use automated decision making or automated processing, it will consult in advance with the DPO to ensure it meets its obligations.

PART B: DATA BREACH

UK GDPR places obligations on the school to report certain breaches of Personal Data to the Information Commissioner's Office (**ICO**) and, in some circumstances, to inform the affected Data Subjects of the breach.

The school has put in place procedures to notify the ICO and inform affected Data Subjects where it is legally required to do so.

All members of Staff are required to familiarise themselves with the procedure for dealing with Personal Data Breaches below, and to comply with the provisions contained in it.

This policy is to be provided to Data Processors who process Personal Data on behalf of the school, who must notify the Data Protection Lead as soon as possible if they become aware of a Personal Data Breach. Failure to do so may breach the processing agreement between the school and the Data Processor and/ or allow the school to terminate that agreement without notice.

If you become aware of or suspect that there has been a Personal Data Breach, you must immediately contact the Data Protection Lead (see below). Do not attempt to investigate the matter yourself.

8. Data Protection Lead

The school's **Data Protection Lead** has overall responsibility for Personal Data Breach notification within the school. The Data Protection Lead:

- is responsible for ensuring breach notification processes are adhered to by all staff;
- is responsible for maintaining the school's Data Breach Register; and
- is the designated point of contact for staff to report Personal Data Breaches.

The Data Protection Lead is Sarah Williams, who can be contacted at:

020 8989 2791
DPL@wansteadhigh.co.uk

Please note that this is a separate position to the Data Protection Officer (**DPO**), (who is responsible for overseeing this Policy and developing data-related procedures and guidelines) However, if you are unable to make contact with the Data Protection Lead in the event of an actual or potential Personal Data Breach, please contact the DPO, who is:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (Option 1, then 1)

9. What is a Personal Data Breach?

A Personal Data Breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data or Special Category Data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive):

- Loss (including accidental loss) or theft of data or equipment on which data is stored (e.g. loss of a school laptop or a paper file).
- Inappropriate access controls allowing unauthorised use or access to data.
- Unauthorised sharing of data.
- Human error (e.g. sending an email or WhatsApp to the wrong recipient).
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.
- Unforeseen circumstances such as a fire or flood.

10. When does a Personal Data Breach need to be reported to the ICO?

The school must notify the ICO of a Personal Data Breach where the breach is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing Personal Data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach is likely to have a significant detrimental effect includes where the breach leads to:

- potential or actual discrimination;
- potential or actual financial loss (e.g. through the release of credit card details);
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (e.g. through the release of non-public identifiers such as passport details);
- the exposure of a sensitive private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly. The Data Protection Lead is responsible for notifying the individuals.

11. What do I do if I know or suspect there has been a Personal Data Breach?

If you become aware of or suspect a Personal Data Breach has occurred or may occur which meets the criteria above, you should, as soon as possible:

- complete a Data Breach Report Form (which can be obtained from the Data Protection Lead (Sarah Williams)); and

- email the completed form to DPL@wansteadhigh.co.uk.

Where appropriate, you should liaise with your line manager about completion of the Data Breach Report Form. Breach reporting is encouraged throughout the school and staff are expected to seek advice from their line manager or the DPO if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. However, you must ensure that this does not materially delay your completion and return of the form to the Data Protection Lead.

If in doubt about whether a Personal Data Breach should be reported to the Data Protection Lead, please report it.

Once reported to the Data Protection Lead, you should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators or investigate further. The Data Protection Lead will acknowledge receipt of the Data Breach Report form and take appropriate steps to deal with the report in collaboration with the DPO.

12. Steps for the Data Protection Lead in the event of a known or suspected Personal Data Breach

Managing and recording the breach

On being notified of a Personal Data Breach or suspected Personal Data Breach, the Data Protection Lead must:

- notify the DPO; and
- take immediate steps to establish whether a Personal Data Breach has in fact occurred.

Where the Data Protection Lead finds that a Personal Data Breach has occurred, they must:

- where possible, contain the breach to prevent further data loss;
- as far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- assess and record the breach in the school's Data Breach Register;
- notify the ICO where required;
- notify data subjects affected by the breach if required;
- notify other appropriate parties to the breach; and
- take steps to prevent future breaches.

Notifying the ICO

The Data Protection Lead must notify the ICO when a Personal Data Breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of whether or not the school is open (i.e. it is not 72 school hours). If the Data Protection Lead is unsure of whether to make a notification, they should consult with the DPO and, where there is still doubt, the assumption must be to notify the ICO.

Where the notification is not made within 72 hours of becoming aware of the breach, the Data Protection Lead will be required to provide written reasons in the ICO notification as to why there was a delay in notifying the matter to the ICO.

Notifying Data Subjects

Where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Lead must notify the affected Data Subjects without undue delay of the breach and provide:

- the name and contact details of the DPO;
- the contact details of the ICO;
- the likely consequences of the data breach; and
- the measures the school has taken, or intends to take, to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Data Protection Lead shall co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities which may be involved (such as the police).

If it would involve disproportionate effort to notify the Data Subjects directly (e.g. where reasonable searches have not found the contact details of those affected, or where there are so many affected Data Subjects that individual contact is not practicable) then the Data Protection Lead must consider alternative means to make those affected aware (e.g. by making a statement on the school website).

Notifying other authorities

The Data Protection Lead, in collaboration with the DPO, must consider whether other parties need to be notified of the breach. These other parties might include:

- insurers;
- parents/carers;
- third parties (e.g. when they are also affected by the breach);
- the Local Authority;
- The police (e.g. if the breach involved theft of equipment or data).

Assessing the Breach

Once initial reporting procedures have been carried out, the Data Protection Lead, in consultation with the DPO and with the assistance of appropriate individuals in the school (eg. the ICT Manager or Network Manager), must carry out investigation into the breach.

The investigation should seek to:

- identify how the breach occurred;
- take any further steps identified to stop or minimise further loss, destruction or unauthorised disclosure of personal data;
- identify ways to recover correct or delete data (e.g. notifying the police if the breach involves stolen hardware or data);
- identify what type of data is involved and how sensitive it is;
- the volume of data affected;
- which Data Subjects are affected by the breach;
- the likely consequences of the breach on affected Data Subjects;
- whether there are there any protections in place to secure the data which has been breached (e.g. encryption, password protection, pseudonymisation);
- what has happened to the data;

- what the data tell a third party about the Data Subject (whether on its own, or when combined with other information already available to a third party, e.g. because it is in the public domain);
- the likely consequences of the breach on the school and its operations;
- whether further issues are likely to materialise; and
- any other wider consequences which may be applicable.

13. Preventing Future Breaches

Following a data breach, the school must consider its security processes with the aim of preventing further breaches. In order to do this, the Data Protection Lead, in collaboration with the DPO, must:

- update the school's Data Breach Register;
- debrief the Governing Body and the Headteacher;
- establish what security measures were in place when the breach occurred;
- assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- consider whether it is necessary to conduct a privacy or data protection impact assessment; and
- consider whether further audits or data protection steps need to be taken.

14. Reporting data protection concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time, and we encourage you to report any concerns (even if they do not meet the criteria of a Personal Data Breach) that you may have to the Data Protection Lead or the DPO. This can help capture risks as they emerge, protect the school from data breaches and keep our processes up to date and effective.

PART C: DATA RETENTION

The school has a responsibility to maintain its records and record-keeping systems. When doing this, the school will take account of the following factors:

- Why it is holding the data, and if it is justified to do so;
- Whether it has a legal duty to keep the data for a set period of time;
- Whether the data is needed to meet Ofsted's requirements;
- Whether that data may need to be shared (eg. with the Local Authority);
- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

This part of the Policy sets out how long employment-related and pupil data will normally be held by the school and when that information will be confidentially destroyed in compliance with UK GDPR and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the school. Parts A and B of this Policy outlines the school's duties and obligations under UK GDPR.

15. Record keeping of Personal Data Processing

The Data Protection Lead is responsible for keeping full and accurate records of the school's data processing activities. These records include:

- The name and contact details of the school;
- The name and contact details of the Data Protection Officer (DPO);
- 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.

16. Record keeping of SARs

A record of all SARs shall be kept by the Data Protection Lead is responsible for keeping a record of all SARs. The record shall include the date the SAR was received, the name of the requester, what data the school sent to the requester and the date of the response.

17. Retention Schedule

Information (hard copy and electronic) will be retained for the period specified in the **Data Retention Schedule at Appendix 1 to this Policy**. When managing records, the school will adhere to the standard retention times listed within that schedule.

Paper records and electronic records will be regularly monitored by the Office Manager under the direction of the Data Protection Lead.

The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

Data types and associated retention periods may be added or updated at intervals between reviews as appropriate.

18. Destruction of records

Where records have been identified for destruction, they should be disposed of in an appropriate way.

All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing Personal Data, or other sensitive information, should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate wastepaper merchant. All electronic information will be deleted.

The school maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate Staff member should record in this list at least:

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising manager.

19. Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. The Data Protection Lead maintains a database of the records sent to the archives. The appropriate Staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

If we are a pupil's final school of compulsory education, we will retain the pupil record for the full retention period as specified in this policy. However, if a pupil transfers to another school before completion of their compulsory education, the file should be sent to their next school. The responsibility for retention then shifts onto the next school. We retain the file for a year following transfer in case any issues arise as a result of the transfer.

20. Retention of Safeguarding Records

Any allegations made that are found to be malicious must not be part of the personnel records. For any other allegations made, the school must keep a comprehensive summary of the allegation made, details of how the investigation was looked into and resolved and any decisions reached. This should be kept on the personnel files of the accused.

Any allegations made of sexual abuse should be preserved by the school for the term of an inquiry by the Independent Inquiry into Child Sexual Abuse. All other records (for example, the personnel file of the accused) should be retained until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer. In 2022, the Independent Inquiry into Child Sexual Abuse (IICSA) concluded and published their final report, leaving a recommendation that all records relating to child sexual abuse should be retained for a period of 75 years.

The ICO has not currently produced guidance or frameworks regarding retention as recommended by the inquiry. Until this has been produced, records will still be retained for a prolonged period as recommended initially by IISCA in order fulfil potential legal duties that a school may have in relation to the inquiry or any further guidance.

21. Transferring information to other media

Where lengthy retention periods have been allocated to records, Staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

22. Responsibility and monitoring

The Data Protection Lead has primary and day-to-day responsibility for implementing this Part of the Policy. The Data Protection Officer (DPO), in conjunction with the Data Protection Lead and the school is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The DPO will consider the suitability and adequacy of this Policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Staff who are line managers at all levels are responsible for ensuring that those reporting to them are made aware of and understand this Policy and to flag to management where they or their teams may need additional training on it to that already provided by the school.

Appendix 1 – Data Retention Schedule

DATA DESCRIPTION	RETENTION PERIOD
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	6 years after employment ceases
Immigration checks	2 years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel records	While employment continues and up to six years after employment ceases (Limitation Act 1980)
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: • Opt-out forms • Records of compliance with WTR	• Two years from the date on which they were entered into • Two years after the relevant period
Disciplinary records	6 years after employment ceases

DATA DESCRIPTION	RETENTION PERIOD
Training	6 years after employment ceases or length of time required by the professional body
Staff training where it relates to safeguarding or other child related training	Date of the training plus 40 years (This retention period reflects that the IICSA may wish to see training records as part of an investigation)
Annual appraisal/assessment records	Current year plus 6 years
Professional Development Plans	6 years from the life of the plan
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.
Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	Until updated plus 3 years
Bonus Sheets	Current year plus 3 years
Time sheets/clock cards/flexi-time	Current year plus 3 years
Pupil Premium Fund records	Date pupil leaves the provision plus 6 years
National Insurance (schedule of payments)	Current year plus 6 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Insurance	Current year plus 6 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Overtime	Current year plus 3 years (Taxes Management Act 1970; Income and Corporation Taxes 1988)
Annual accounts	Current year plus 6 years
Loans and grants managed by the school	Date of last payment on the loan plus 12 years
All records relating to the creation and management of budgets	Life of the budget plus 3 years

DATA DESCRIPTION	RETENTION PERIOD
Invoices, receipts, order books and requisitions, delivery notices	Current financial year plus 6 years
Student Grant applications	Current year plus 3 years
Pupil Premium Fund records	Date pupil leaves the school plus 6 years
School fund documentation (including but not limited to invoices, cheque books, receipts, bank statements etc.)	Current year plus 6 years
Free school meals registers (where the register is used as a basis for funding)	Current year plus 6 years
School meal registers and summary sheets	Current year plus 3 years
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
School Development Plans	3 years from the life of the plan
Visitors Book and Signing in Sheets	6 years
Newsletters and circulars to staff, parents and pupils	1 year (and the school may decide to archive one copy)
Minutes of Senior Management Team meetings	Date of the meeting plus 3 years or as required
Reports created by the Headteacher or the Senior Management Team.	Date of the report plus a minimum of 3 years or as required
Records relating to the creation and publication of the school prospectus	Current academic year plus 3 years
Health and Safety Records	
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years
Health and Safety Policy Statements	Life of policy plus 3 years
Any records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relating to the incident are held on personnel file
Accident reporting records relating to individuals who are under 18 years of age at the time of the incident	Until the child reaches the age of 21

DATA DESCRIPTION	RETENTION PERIOD
Accident reporting records relating to individuals who are over 18 years of age at the time of the incident	Accident book should be retained 3 years after last entry in the book. (Social Security (Claims and Payments) Regulations 1979; Social Security Administration Act 1992; Limitation Act 1980)
Fire precaution logbooks	Current year plus 3 years
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record (Control of Substances Hazardous to Health Regulations (COSHH); Control of Asbestos at Work Regulations)
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Governing Body Documents	
Instruments of government	For the life of the school
Meetings schedule	Current year
Minutes – principal set (signed)	Generally kept for the life of the organisation
Agenda – principal copy	Where possible the agenda should be stored with the principal set of the minutes
Agenda – additional copies	Date of meeting
Policy documents created and administered by the governing body	Until replaced
Register of attendance at full governing board meetings	Date of last meeting in the book plus 6 years
Annual reports required by the Department of Education	Date of report plus 10 years
Records relating to complaints made to and investigated by the governing body or head teacher	Major complaints: current year plus 6 years. If negligence involved: current year plus 15 years. If child protection or safeguarding issues are involved: current year plus 40 years.

DATA DESCRIPTION	RETENTION PERIOD
Correspondence sent and received by the governing body or head teacher	General correspondence should be retained for current year plus 3 years
Records relating to the terms of office of serving governors, including evidence of appointment	Date appointment ceases plus 6 years
Register of business interests	Date appointment ceases plus 6 years
Records relating to the training required and received by governors	Date appointment ceases plus 6 years
Records relating to the appointment of a clerk to the governing body	Date on which clerk appointment ceases plus 6 years
Governor personnel files	Date appointment ceases plus 6 years
Pupil Records	
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission
Proof of address supplied by parents as part of the admissions process	Current year plus 1 year
Admissions register	Entries to preserved for 6 years from date of entry (working together to improve school attendance, Section 36, 2024 statutory guidance)
Pupil Record	Secondary – until the child reaches the age of 25 (Limitation Act 1980)
Attendance Registers	6 years from the date of entry (working together to improve school attendance, Section 36, 2024 statutory guidance)
Correspondence relating to any absence (authorised or unauthorised)	Current academic year plus 2 years (Education Act 1996)
Special Educational Needs files, reviews and Education, Health and Care Plan, including advice and information provided to parents regarding educational needs and accessibility strategy	Date of birth of the pupil plus 31 years (Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan). (Children and Family's Act 2014; Special Educational Needs and Disability Act 2001)
Child protection information (to be held in a separate file).	DOB of the child plus 25 years then review Note: These records will be subject to any instruction given by IICSA
Exam results (pupil copy)	3 years from the date the results are released
Examination results (school's copy)	Current year plus 6 years

DATA DESCRIPTION	RETENTION PERIOD
Allegations of sexual abuse	For the time period of an inquiry by the Independent Inquiry into Child Sexual Abuse
Records relating to any allegation of a child protection nature against a member of staff	Until the accused normal retirement age or 10 years from the date of the allegation (whichever is the longer)
Consents relating to school activities as part of UK GDPR compliance (for example, consent to be sent circulars or mailings)	Consent will last whilst the pupil attends the school
Pupil's work	Where possible, returned to pupil at the end of the academic year (provided the school have their own internal policy to this effect). Otherwise, the work should be retained for the current year plus 1 year
Mark books	Current year plus 1 year
Schemes of work	Current year plus 1 year
Timetable	Current year plus 1 year
Class record books	Current year plus 1 year
Record of homework set	Current year plus 1 year
Photographs of pupils	For the time the child is at the school and for a short while after. Please note select images may also be kept for longer (for example to illustrate history of the school).
Parental consent forms for school trips where there has been no major incident	End of the trip or end of the academic year (subject to a risk assessment carried out by the school)
Parental permission slips for school trips where there has been a major incident	Date of birth of the pupil involved in the incident plus 25 years. Permission slips for all the pupils on the trip should be retained to demonstrate the rules had been followed for all pupils
Other Records	
Emails	3 years
CCTV	1 Calendar Month[2]

[2] Where an incident or issue occurs, the CCTV Policy provides that footage may be retained for longer – **refer to the CCTV Policy.**

DATA DESCRIPTION	RETENTION PERIOD
Privacy notices	Until replaced plus 6 years
Inventories of furniture and equipment	Current year plus 6 years
All records relating to the maintenance of the school carried out by contractors or employees of the school	Whilst the building belongs to the school
Records relating to the letting of school premises	Current financial year plus 6 years
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	Current year plus 6 years then review
Referral forms	While the referral is current
Contact data sheets	Current year then review, if contact is no longer active then destroy

Appendix 2 – Subject Access Requests (SARs) Procedure

1. Introduction - Data Subject rights of access

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.

This Procedure provides guidance for:

- Staff on how data SARs should be handled; and
- all individuals on how to most effectively make a SAR to the school.

Failure to comply with the right of access under UK GDPR puts both Staff and the school at potentially significant risk and so the school takes compliance with this Procedure very seriously.

A. MAKING A SAR TO THE SCHOOL

2. How to make a SAR to the school

Whilst there is no requirement to do so, we encourage any individuals who wish to make a SAR to the school to:

- make the request in writing; and
- detail exactly the Personal Data being requested, including who the Data Subject(s) is, any relevant time periods, and other identifying information.

Please use the form at Annex I (**Subject Access Request Form**) to make your SAR where possible.

This allows the school to easily recognise that you wish to make a SAR and to understand the nature and scope of your request.

If the request is unclear/vague, or we need more detail in order to identify the data which is the subject of the request, we may need to clarify with you and others the scope of the request, which may in turn delay the start of the time period for dealing with the request.

3. School closure periods

The school may not be able to respond to SARs received during or just before school closure periods (eg. School holidays) within the one calendar month response period, including because the school will be closed and there will likely be no-one on site who is able to respond to the SAR, and/or because relevant Personal Data may be held by individuals who are not on site and do not review emails during this period. As a result, it is unlikely that your request will be able to be dealt with during this time.

If your SAR arrives when the school is closed, we may not be able to acknowledge your SAR until it is received when the school reopens. However, if we can acknowledge the request, we may still not be able to deal with it until the school reopens. The school will endeavour to comply with SARs as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide make your SAR during term time and not during/close to closure periods.

B. RECEIPT OF A SAR BY THE SCHOOL

4. How to recognise a SAR

A SAR may be a request received from an individual, or from someone acting with the authority of or on behalf of an individual (eg. a solicitor, or a parent making a request for information relating to their child), seeking:

- confirmation as to whether the school processes personal data about them (or the person on whose behalf they are acting);
- access to that personal data; and/or
- certain other supplementary information (see the list in the introduction to this Procedure for more examples).

A SAR is equally valid whether it is made verbally (e.g. during a meeting telephone conversation) or writing (there is no prescribed form – this can be done by letter, email, WhatsApp, etc) or;

The request may refer to UK GDPR and/or to 'data protection' and/or to 'personal data' - but it 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' would be sufficient to constitute a SAR and should be treated as such.

Note, however, that while a SAR may be phrased in broad terms, a Data Subject (or someone authorised to act on their behalf) is generally only entitled to access their own Personal Data and not information relating to other people.

5. What to do if you receive a SAR

All requests should be immediately directed to the Data Protection Lead. There are limited timescales within which the school must respond to a SAR 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.

The Data Protection Lead is Sarah Williams, who can be contacted at:

020 8989 2791
DPL@wansteadhigh.co.uk

The Data Protection Lead will work with the DPO in order to appropriately respond to the request.

6. Acknowledging the SAR

On receiving a SAR, the Data Protection Lead will direct the school to acknowledge the request as soon as possible and inform the requester of the statutory deadline (one calendar month) for the school to respond to the SAR.

In addition to acknowledging the request, the school may ask for:

- proof of identification (if needed);
- further clarification about the requested information;
- if it is not clear where copies of information are to be sent, the address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The Data Protection Lead will work with the DPO in order to create the form of acknowledgment.

7. **Verifying the identity of the requester / Requesting clarification of the SAR**

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 doubt as to the identity of the requester, evidence of identity may be established by production of a suitable document or combination of documents, such as passport, driving licence, recent utility bill with current address, birth/marriage certificate, credit card or mortgage statement.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

If an individual is requesting a large amount of data, or if the request is not clear on what is being requested, the school may ask the requester for more information for the purpose of clarifying the request. However, the requester must never be asked why the request has been made. The school shall let the requestor know as soon as possible where more information is needed before the school can respond to the SAR.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if it does not receive the additional information.

8. SARs made by third parties

The school need to be satisfied that any third party making a SAR (i.e. a person who is not the Data Subject of the Personal Data being requested) is authorised to act on behalf of the individual, and it is the third party's responsibility to provide evidence of this authorisation. This might be a written authority given by the Data Subject 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.

9. **SARs made on behalf of children**

When a SAR is made on behalf of a child or 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 shall assess if the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, the school should take into account, among other things:

- the child's level of maturity and their ability to make decisions of this nature;
- 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;
- any consequences of allowing those with parental responsibility access to the child's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child if individuals with parental responsibility cannot access this information; and
- any views the child has on whether those with parental responsibility for them 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 of 12 years of age or older, 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 child's Personal Data directly to the child.

The form at Annex II (**Pupil Consent to Sharing Personal Data**) is to be used to consent from a child to provide their Personal Data to others.

The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information (e.g. if it is likely to cause detriment to the child).

10. Fee for responding to a SAR / Refusing to respond to a SAR

The school will usually provide a response to a SAR free of charge.

The school can refuse to comply with a SAR if it is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature. If a SAR is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to respond to the SAR; or
- refuse to deal with the SAR.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the SAR. If deciding to charge a fee, the school will inform the requester why this is considered to be the case and that the school will charge a fee for complying with the request to cover its administrative costs.

A fee may also be requested for providing repeat copies of the same information. In these circumstances a reasonable fee will be charged, taking into account the administrative costs of providing the information.

If a fee is requested, the time period for responding to the SAR begins when the fee is received by the school.

11. **Time period for responding to a SAR**

The school has one calendar month to respond to a SAR. This will run from the day that the SAR 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.

In circumstances where the school had reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and, in the case of a third-party requester, the written authorisation of the Data Subject has been received.

The time period for responding 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 SAR. The DPO must always be consulted in determining whether a request is sufficiently complex so as to extend the time period for responding.

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

12. Information to be provided in response to a SAR

The Data Subject is entitled to receive access to the Personal Data about them which we process, together with the following information:

- the purpose for which we Process the Personal Data;
- the recipients or categories of recipient to whom the Personal Data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the Personal Data will be stored, or, if not possible, the criteria used to determine that period;

- the fact that the individual has the right:
    - to request that the school rectifies, erases or restricts the processing of their Personal Data;
    - to object to its Processing;
    - to lodge a complaint with the ICO;
    - where the Personal Data has not been collected from the individual, to be provided with any information available regarding the source of the Personal Data;
    - any automated decision the school has taken about them, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them.

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 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 Personal Data in existence at the time the request was received. However, as the school has one month in which to respond, it is allowed to take into account any amendment or deletion made to the Personal Data between the time the SAR 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.

Therefore, the school is 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 Personal Data to avoid supplying it in response to a SAR.

13. **How to locate Personal Data**

The Personal Data to be provided in response to a SAR may be located in a number of places. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the school may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The school should search these systems using the Data Subject's name, employee number or other personal identifier as a search determinant.

14. **Exemptions to the right of access**

There are circumstances where information requested in a SAR can be withheld. These specific exemptions and requests should be considered on a case-by-case basis, in consultation with the DPO.

Protection of third parties

The school will consider whether it is possible to redact information which is responsive to a SAR so that it does not identify those third parties. If their data cannot be appropriately redacted (eg. after redaction it is still obvious who the data relates to) then the school does not have to disclose the Personal Data to the extent that doing so would involve disclosing information relating to the third party (including information identifying the third party as the source of the Personal Data) unless:

- the third party has consented to the disclosure; or
- it is reasonable to comply with the request without the third party's consent.

In determining whether it is reasonable to disclose the information without the third party's consent, all of the relevant circumstances are to be taken into account, including:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the third party;
- any steps taken to seek consent from the third party;
- whether the third party is capable of giving consent; and
- any express refusal of consent by the third party.

The school will need to decide whether it is appropriate to disclose the information in each case. This decision will involve balancing the Data Subject's right of access against the third party's rights. If the third-party consents to the school disclosing the information that identifies 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. The DPO should be consulted in relation to any such decision.

Other exemptions to the right of access

The exemptions described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

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.

Confidential references: The school does not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service.

This exemption does not apply to confidential references that the school receives from an external source. However, in this situation, granting access to the reference may disclose the Personal Data of a third party

(ie. 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.

Legal professional privilege: The school does not have to disclose any Personal Data which is subject to legal professional privilege. If in doubt, the school should seek legal advice on whether data is privileged.

Management forecasting: The school does not have to disclose any Personal Data Processed for the purposes of management forecasting or management planning or to assist in the conduct of any business or any other activity.

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.

15. Record Keeping

A record of all SARs shall be kept by the Data Protection Lead. The record shall include the date the SAR was received, the name of the requester, what data the school sent to the requester and the date of the response.

Annex I to the Subject Access Requests (SARs) Procedure:

Subject Access Request Form

You have a right to receive a copy of the personal data and associated information that we hold about you, or about someone whom you are authorised to act for (e.g. a child under 12 for whom you have parental responsibility).

Please complete this form if you wish to make a request for personal data held by the school. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

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

DPL@wansteadhigh.co.uk

Section 1: Details of the Data Subject

Please provide the details of the Data Subject (ie. you, or another person whose personal data you are requesting).

If you are not the Data Subject and you are making a request on behalf of someone else, please fill in the details of the Data Subject below and not your own, please also complete Section 4 below.

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

Section 2: Personal data requested

Please describe in as much detail as possible what personal data you are requesting access to (*if you only want to know what information is held in specific records (and do not necessarily wish to have access to it or copies of it), please indicate this).*

Please provide as much detail as possible to enable to us to identify the personal data:

- What capacity or context was the data provided to the school/is the data held by the school?
- What time period of personal data are you looking for? If you do not know exact dates, please give the year(s) that you think may be relevant.
- Are there additional names to that of the Data Subject which may assist us?
- What categories of data are you looking for? Are you looking for data relating to a specific case?
- Are you requesting just paper records, or just electronic records, or both?

If you are, or have been employed by school and are seeking personal data in relation to your employment please provide details such as:

- your staff number;
- your role and department;
- your dates of employment;
- your line manager(s).

We require proof of the Data Subject's identity before we can disclose personal data. Please provide a copy of one or more documents - such as your birth certificate, passport, driving licence or official letter addressed to you at your address (eg. bank statement, recent utility bill or council tax bill) - which together include your:

- name;
- date of birth; and
- current address.

If you have changed your name, please supply relevant documents evidencing the change.

If you are not the data subject and you are making a request on behalf of someone else, please provide proof of the data subject's identity below and not your own, please also complete Section 4 below.

I am enclosing copies of the following documents as proof of my identity (please tick the relevant box(es)): ☐ Birth certificate ☐ Driving licence ☐ Passport ☐ An official letter addressed to me at my address

Section 3: Receipt of the response

I wish to receive the school's response to my request for personal data: ☐ By post* ☐ By email (or file sharing site if the data is too large for email) ☐ Collect the response in person from the school ☐ View the information requested only ☐ Go through the information requested with a member of Staff *Please be aware that if you wish us to post the information to you, we will 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 also note that if it is not practical or proportionate to make hardcopies of electronic information, then we may need to send this to you in electronic format.

Section 4: Details of the data subject's representative (if applicable)

If you are not the data subject but are acting on their behalf, please fill in this section.

Title	
Surname/ Family Name	
First Name(s)/Forenames	

Date of Birth	
Address	
Post Code	
Phone Number	

You will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Please provide a copy of one or more documents - such as your birth certificate, passport, driving licence or official letter addressed to you at your address (eg. bank statement, recent utility bill or council tax bill) - which together include your:

- name;
- date of birth; and
- current address.

If you have changed your name, please supply relevant documents evidencing the change.

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

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter addressed to me at my address

What is your relationship to the Data Subject? (eg., parent, carer, legal guardian, legal representative)

I am enclosing the copies of the following documents as proof that I am authorised to make this request behalf of the data subject:

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

Annex II to the Subject Access Requests (SARs) Procedure:

Pupil Consent to Sharing Personal Data Form

Guidance for use: This form is used to seek consent from pupils for sharing of their Personal Data with others who may request it (e.g. their parent or carer). The form may be used only in respect of a child who the school considers has sufficient mental capacity and ability to understand a subject access request (SAR) and the concept of data rights and consent.

Consent to Sharing Personal Data

All schools collect a lot of information about their pupils. This includes information which is known as 'personal data', which is information which is personal to you, or can identify you, such as your full name, address, medical information and behaviour records.

We have received a request from [NAME] who has asked for a copy of your personal data. You have rights in respect of the personal data that the school holds about you. We can only share your personal data with this person if you say we can share it, and we can only share with this person the information that the law says we can.

Your consent

This form asks you to confirm whether or not you give the school your consent to share your personal data with the person named above.

We will explain what this all means before you make a decision. Remember to ask any questions if you are not sure.

Please confirm how you would like us to handle your personal data by ticking ONE of the boxes below:

□ I would like a copy of my personal data to be provided to the person named above.

OR

□ I would like a copy of my personal data to be provided directly to me (and not to the person named above).

OR

□ I do not want a copy of my personal data to be disclosed to the person named above or to me.

Your signature: _____

Your name: _____

Date: _____

Please return your completed form to Ms S Williams (School Business Manager).