PINNER
HIGH SCHOOL

Policy	Data Protection Policy
Date of Review	April 2026
Reviewed By	Data Manager and Head of Operations
Date of Approval	*Pending*
Approved By	LGB
Date of Next Review	April 2028
Statutory/Non Statutory	Statutory
Website/Non Website	Website

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of format, including data processed on school-owned equipment and personal devices used for school business.

2. Legislation and guidance

This policy complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It takes account of guidance and Codes of Practice issued by the Information Commissioner's Office (ICO).

Following the UK's exit from the European Union, the school primarily operates under the UK GDPR. However, where the school processes personal data relating to individuals within the European Economic Area (EEA), it will ensure compliance with the EU GDPR (Regulation (EU) 2016/679), where applicable.

In relation to biometric data, the school complies with the Protection of Freedoms Act 2012 (sections 26–28), including the requirement to obtain written parental consent.

The use of surveillance systems, including CCTV, is carried out in accordance with the ICO's guidance on video surveillance and is subject to regular Data Protection Impact Assessments (DPIAs).

Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs

	• Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Subject Access Request (SAR)	A formal or informal request by or on behalf of an individual to see the personal data the school holds about them.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, trustees, visitors and others, and therefore is a data controller.

Harrow Academies Trust, of which the school is a part, is registered as a data controller with the ICO. The registration number is ZA 183398. The school commits to maintaining a valid registration

5. Roles and responsibilities

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

5.1 Harrow Academies Trust and the Local Governing Body

Harrow Academies Trust has overall responsibility for ensuring that our school complies with all relevant data protection obligations.The Local Governing Body has delegated supervisory responsibility **for day-to-day oversight, while the Trust remains the ultimate legal entity accountable for compliance.**

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for advising on the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the Local Governing Body and, where relevant, report their advice and recommendations on school data protection issues.

The DPO is also a point of contact for individuals whose data the school processes, and for the ICO.

We, alongside the consortium of Harrow High Schools of which we are part, have appointed an external DPO since Autumn 2018: **Judicium Consulting Limited, 72 Canon Street, London, EC4N 6AE**

5.3 Representative of the Data Controller on a day to day basis

The school Data Manager, supported by the Head of ICT, Rakhee Jotangia, and the Head of Operations, Hilary Ford, shall act as the representative of the data controller on a day-to-day basis.

5.4 All Staff

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Data Manager and/or Head of Operations in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

- Staff must contact the Head of Operations, the Head of ICT or the Data Manager immediately if:
    - They suspect a personal data breach has occurred.
    - They believe this policy is being willfully disregarded.
    - They identify a high risk to the privacy of individuals."

6. Data protection principles

The school **adheres to** the seven Data Protection Principles set out in Article 5 of the UK GDPR. These principles form the basis of our internal procedures and compliance framework.

Personal data shall be:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary (Data Minimisation).
4. Accurate and regularly reviewed for accuracy; inaccurate data shall be erased or rectified without delay.
5. Kept in a form which permits identification of data subjects for no longer than is necessary, in strict accordance with the School's Data Retention Schedule.
6. Processed in a way that ensures integrity and confidentiality, using technical and organisational measures to ensure protection against unauthorised or unlawful processing and accidental loss.
7. Accountability: The school is responsible for, and must be able to demonstrate compliance with, all the principles listed above.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

At the point of admission to the school as a student or induction as an employee, governor, or trustee, the school shall provide individuals with a privacy notice. Privacy notices will also be published on the school website. Any material changes to how data is processed will be communicated directly to data subjects in an appropriate and proportionate way.

The school will only process personal data where it has a lawful basis to do so under the UK General Data Protection Regulation (UK GDPR). The lawful bases are:

- **Contract** – where processing is necessary for the performance of a contract with an individual, or to take steps at their request before entering into a contract
- **Legal obligation** – where processing is necessary for compliance with a legal obligation to which the school is subject
- **Vital interests** – where processing is necessary to protect someone's life
- **Public task** – where processing is necessary for the school to perform a task carried out in the public interest or in the exercise of its official authority
- **Legitimate interests** – where processing is necessary for the legitimate interests of the school or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual. This basis will only be used where the processing does not form part of the school's public task
- **Consent** – where the individual (or, where appropriate, their parent or carer) has given clear, freely given consent

For special categories of personal data, as defined in the UK GDPR and Data Protection Act 2018 and summarised at appendix 2 to this policy, we will also have to satisfy one of the additional specific special category conditions set out in appendix 2.

Most aspects of a school's data processing will be on the lawful basis that the data needs to be processed so that the school, as a public authority, can perform a task in the public interest and carry out its official functions or to fulfill a contract with an individual. But where we will rely specifically on the sixth lawful basis, **consent,** as a basis for processing, we will follow the principles below in order to obtain the correct consent, respecting both a pupil's increasing maturity and the valued triangular partnership between school, pupil and parent.

For pupils aged 13 and over, the school will assess the individual's **capacity to understand** the implications of the specific data processing (Competency Assessment).

- Where a pupil is deemed competent, their consent (or lack of) will usually take precedence over that of their parent

- The school will maintain a record of whether a pupil was deemed competent (or not) for any high-stakes data processing, and of their consent (or non consent) in that scenario..
- **Conflict Resolution:** If a competent pupil consents but a parent objects, or vice versa, the pupil's legal right to control their data will generally prevail under the UK GDPR, unless a specific safeguarding override applies

7.2 Limitation, minimisation and accuracy

Data Minimisation The school complies with the principle of data minimisation. Personal data collected will be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Change of Purpose: If the school intends to use personal data for a purpose other than that for which it was originally collected, we will conduct a **Compatibility Assessment**. If the new purpose is not compatible with the original purpose, we will either identify a new lawful basis or seek fresh, explicit consent.

Processing Restrictions: Staff are strictly prohibited from processing personal data for personal use or outside the formal scope of their employment. All processing must occur within school-approved systems; the creation of 'shadow' or unofficial data records is a violation of this policy.

Retention and Disposal: Personal data **must** be deleted or anonymized once the retention period specified in the **School Records Management & Retention Schedule** has expired. The school formally **adopts the retention periods** set out in the *Information and Records Management Society's* (IRMS) Toolkit for Schools. Anonymization must be performed such that the individual is no longer identifiable by any reasonable means.

8. Sharing personal data

We will not share personal data with anyone else without consent unless the law and our policies allow us to.

Examples of with whom we may share data include (but are not limited to) the following:

- A pupil's parent/carer or (in limited circumstances) a staff member's family or representatives
- A local authority, the Department for Education, Ofsted or other statutory body, to meet our legal obligations to share certain information such as census, safeguarding, exclusions, training, or inspection data
- Our trustees and governors
- Our auditors
- Educators and examining bodies
- Suppliers and service providers to enable them to provide services and support to pupils or the school
- Professional advisers and consultants
- Charities and voluntary organisations
- HR, Pension, Tax and employment-related agencies
- Professional bodies
- Schools that the pupil attends after leaving us
- Health and social welfare professionals and organisations, emergency services, police forces, courts, tribunals (especially for safeguarding, safety or legal reasons)

Where the school uses third-party data processors (such as IT systems providers, cashless catering systems, school apps / communication platforms, CCTV hosting providers, external HR/payroll software providers), it will ensure that a written contract is in place that meets the requirements of Article 28 of the UK

GDPR. The school will only appoint processors that can demonstrate appropriate technical and organisational measures to ensure the security and protection of personal data.

International Transfers: We will not transfer personal data to a country or territory outside the **United Kingdom** unless:

1. That country is covered by a **UK Adequacy Regulation**.
2. The transfer is governed by the **International Data Transfer Agreement (IDTA)** or the **UK Addendum** to the European Commission's Standard Contractual Clauses (SCCs).
3. A **Transfer Risk Assessment (TRA)** has been completed to ensure the data has an essentially equivalent level of protection to that in the UK."

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Subject access requests should be made to the Headteacher's PA (info@pinnerhighschool.org). There is a form on which such a request may be made although it is not necessary to make it on this form. If staff receive an enquiry which is or may be a subject access request they should refer it promptly to the Headteacher's PA and the Head of Operations.

9.2 Responding to subject access requests

Where a pupil is deemed old enough to understand and make their own decisions, which as discussed above will generally be around the age of 13 but will be determined on a case by case basis, it will usually be appropriate for us to seek the child's consent to our complying with any subject access request made by a parent, or for the child to make the subject access request on their own behalf.

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond as soon as practicable and within 1 month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within 3 months of receipt of the request where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension of time is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.3 Other data protection rights of the individual

Individuals have the following additional rights, subject to legal limitations:

- **Right to Rectification:** We will correct inaccurate personal data without undue delay.
- **Right to Erasure/'Right to be Forgotten'**: This right applies where data is no longer necessary or consent is withdrawn. Note: This right does not typically apply to data the school is legally required to keep (e.g., safeguarding records or attendance registers).
- **Right to Restriction**: Individuals can request we 'freeze' data processing while a dispute is resolved.
- **Right to Object**: Individuals may object to processing based on 'Public Interest.' The school will stop such processing unless we can demonstrate compelling legitimate grounds that override the individual's interests.
- **Right to Data Portability**: This applies only to data provided by the individual and processed by consent or contract. We will provide this in a machine-readable format (e.g., CSV or pdf or XLS).

10. Parental requests to see the educational record

A parent's request to access their child's educational record will be considered in accordance with our compliance with GDPR and related legislation and is likely to be treated analogously to a subject access request.

11. Biometric recognition systems

When we use pupils' biometric data as part of an automated biometric recognition system (for example, if pupils are able to use finger prints to pay for school meals instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified that we have a biometric recognition system in place before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a pin code.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and if they do we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they would prefer. Staff and other adults can also withdraw consent at any time and, if so, the school will delete any relevant data already captured.

Note: at the present time, school meals are paid for using a pin code system and the fingerprint system used previously is not in operation. Were it to be resumed, the procedures above would be applicable so this section of our policy has been kept in place.

12. CCTV

We use CCTV in school. We adhere to the ICO's code of practice for the use of CCTV and we have a CCTV policy in place, reviewed by the Head of IT and Network Manager from time to time as appropriate.

13. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos of their child to be used for communication, marketing and promotional materials. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will take all reasonable steps to delete the photograph or video and not distribute it further.

14. Data security and storage of records

We will protect personal data and use our best endeavours to keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. We will do this by means of policy, procedure, training and monitoring.

15. Personal data breaches

The school will use our best endeavours to ensure that there are no personal data breaches.

In the event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will take advice from our external DPO and will, if so advised, report the data breach to the ICO within 72 hours.

16. Training

All staff and governors **shall receive appropriate data protection training and be bound by this and other relevant policies and procedures around data protection and ICT acceptable use.** The school will maintain a **Central Training Log** as evidence of compliance.

This log will record the date of training, the content covered, and a record of successful completion for every individual."

17. Monitoring arrangements

The school as data controller is responsible for monitoring and reviewing this policy, with advice and guidance from the DPO as appropriate.

This policy will be reviewed **every 2 years** and approved by the local governing body.

Head of Operations, April 2026

Appendix 1: Privacy Notices (April 2026)

Privacy Notice: Pupils

For a simplified summary of this Privacy Notice, please see the end of this document.

Under UK data protection law, individuals have a right to be informed about the collection, purposes, and storage of their personal data. We fulfill this requirement through this privacy notice, which serves as a definitive statement of our processing activities.

This notice applies to all personal data processed by the school, whether collected directly from the data subject or obtained from third parties (such as the Department for Education or previous educational providers)

As Data Controller, Pinner High School is legally responsible for ensuring that your personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Our Data Protection Officer is **Judicium Consulting Limited** (please see below for contact details).

The personal data we hold

Personal data that we may collect, use, store and (when appropriate) share about pupils includes:

- Personal identifiers such as name, unique pupil number, contact and emergency contact details and preferences, date of birth, siblings, copies of identification documents
- Characteristics such as ethnic background, languages, eligibility for free school meals
- Assessment, attainment, curricular and special educational needs information including information provided by previous schools and external professionals
- Extra-curricular records including involvement in sporting and enrichment activities, school trips and excursions and positions of responsibility
- Medical, welfare, social care and safeguarding information including medical advice, dental and health records, allergy, medication and dietary requirements, involvement of external professionals and agencies, care and family arrangements, relevant court orders
- Pastoral and behavioural information including attendance and exclusion records
- Photographs including by way of electronic school management records and records of school activities and events
- Biometric data used as part of the school's cashless payment system
- CCTV images on site

This data may be provided by pupils, parents/carers, generated internally or received from external organisations, including other schools, local authorities, related agencies or the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Make appropriate pastoral and welfare provision
- Ensure the safe and orderly running of the school
- Communicate with parents/carers and pupils
- Administer applications, admissions and appeals
- Comply with the laws which require us to collect and pass certain pupil data to other bodies concerned with education and/or children
- Manage, assess and promote the quality of our provision

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation, including our legal duty to educate pupils under the Education Act 1996, and to provide related services.
- We need to perform a task carried out in the public interest or in the exercise of an official authority vested in us

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent
- We need to protect the vital interests of the data subject or another person

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

We collect pupil data from pupils, parents/carers, our own performance of services, and from external organisations, including other schools that pupils have attended, local authorities, related agencies and the Department for Education.

Pupil data is important for the school operations and fulfilment of its functions. Whilst the majority of information we collect about pupils to this end is routine and/or mandatory, there is some information that you can decline to provide. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional.

How we store this data

We retain pupil data only for as long as is necessary to fulfill our statutory duties.

- **Standard Educational Records:** Essentially we keep pupil data from the time a pupil is offered a place and/or admitted to the school, whilst they are attending our school and for a limited time beyond their attendance, for practical reasons and in order to comply with our legal obligations.
- **Safeguarding Records:** Retained in accordance with statutory guidance
- **Admissions Data (Unsuccessful):** Retained for one academic year after the appeals process has concluded.

Revised Storage and Security Statement

Personal data is stored within our School Information Management System (Arbor) and other secure, school-approved electronic platforms (including cloud-based providers). Where cloud storage is used, we ensure that data is stored on servers within the **United Kingdom or the EEA**, or under an approved international data transfer mechanism. We maintain robust technical security, including encryption and multi-factor authentication, verified by our external IT security partners, to protect against unauthorized access or loss.

Hard copy records are stored in secure, restricted access locations.

Data sharing

We do not share information about pupils with any third party without consent unless the law and our policies allow us to. Subject to this, we may share pupil data with

- A pupil's parent/carer
- Our local authority or a pupil's home local authority, if different, to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions and information to allow local authorities to discharge post-13 education and training responsibilities
- The Department for Education, to meet our legal obligations to file census data pursuant to regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.
- Our trustees and governors
- Our auditors
- Ofsted
- Educators and examining bodies
- Suppliers and service providers to enable them to provide the service and support to pupils or the school
- Health and social welfare professional and organisations
- Professional advisers and consultants
- Coaches and trip providers
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Schools that the pupil attends after leaving us

Parents' and pupils' rights regarding personal data

Under data protection legislation, parents and pupils have the right to request access to information we hold about them. If you would like to make a request, please contact the Headteacher's PA, contact details below.

You also have the right to

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

Concerns and contacts

- To make a request to access your/your child's personal data, please contact the **Headteacher's PA,** (vfairweather@pinnerhighschool.org)

- If you have any queries, concerns or complaints, please contact our **Data Protection Officer, Data Protection Officer, Judicium Consulting Limited, 72 Canon Street, London, EC4N 6AE**, (dataservices@judicium.com)

- If you remain concerned, you can contact the **Information Commissioner's Office,** (https://ico.org.uk/concerns/)

Summary of this Privacy Notice

1. What is a Privacy Notice?

A privacy notice explains how **Pinner High School** looks after information we hold about you. Under the law, you have a right to know what information we collect, why we need it, and how we keep it safe.

2. Who is in charge of your information?

The school is the "Data Controller," meaning we are responsible for your data. We have a **Data Protection Officer** - a company called Judicium Consulting Limited who advise us how to ensure we follow the rules.

3. What information do we have about you?

We hold things like:

- **The Basics:** Your name, birthday, and address.
- **School Life:** Your grades, attendance, and any extra clubs you join.
- **Your Wellbeing:** If you have allergies, health needs, or things that help us keep you safe.
- **Tech & Security:** Photos of school events, CCTV images for safety, and fingerprint data if you use our "cashless" lunch system.

4. Why do we need it?

Mainly, we use this information to:

- Help you learn and track your progress.
- Look after your health and happiness (pastoral care).
- Keep the school running safely and talk to your parents/carers.

5. Is it okay for us to use your information?

By law, we usually don't need permission as such, because we have a legal duty to educate you. Sometimes we use information because it's in the "public interest" to run a good school. If we ever need your specific **consent** for something optional, we will ask you clearly, and you can say no at any time.

6. Who do we share it with?

We don't just give your information away. We only share it when the law says we must, such as with:

- Your parents or carers.
- The Department for Education and local councils.
- People like school inspectors (Ofsted) or your next school if you move.

7. How do we keep it safe?

Most of your information is stored securely, including in a secure digital system called Arbor. We use high-tech security like encryption and passwords to make sure nobody who shouldn't see it can get to it. We only keep your information for as long as we legally need to.

8. Your Choices (Your Rights)

You have the right to:

- Ask to see the information we have about you.
- Ask us to fix a mistake if your information is wrong.
- Object if you think we are using your data in a way that causes you distress.

Please speak to your Form Tutor, Head of Year or any trusted adult in school if you require more information about your data or your right over it.

Privacy Notice: staff, contractors, agency workers, consultants, volunteers, trustees, governors, job applicants, visitors

Under UK data protection law, individuals have a right to be informed about the collection, purposes, and storage of their personal data. We fulfill this requirement through this privacy notice, which serves as a definitive statement of our processing activities.

This notice applies to all personal data processed by the school, whether collected directly from the data subject or obtained from third parties (such as the Department for Education or previous educational providers)

As Data Controller, Pinner High School is legally responsible for ensuring that your personal data is processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Our Data Protection Officer is **Judicium Consulting Limited** (please see below for contact details).

The personal data we hold

We process data relating to those we employ or otherwise engage to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes:

- Personal identifiers such as name, teacher reference number, contact and emergency contact details and preferences, date of birth, marital status and gender
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information provided by or on behalf or relating to you as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, flexible working requests, training records and professional memberships
- DBS information to demonstrate compliance with Keeping Children Safe in Education (actual certificates are not retained) and a copy of identity information for processing DBS certification
- Performance information such as performance manage records and outcomes of any disciplinary, capability and/or grievance procedures
- Absence records
- Accident reporting and records relating to accident/injury at work
- Photographs
- Data about your use of the school's information and communications system
- CCTV images

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data, for example:

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records
- Biometric data used as part of the school's cashless payment system

In many cases, you have the right to choose whether to share this sort of information with us. See further below on this.

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Inform our recruitment and retention policies and decisions and to facilitate safe recruitment
- Determine your terms of employment, to deliver them and to enable you to be paid and receive relevant benefits
- Comply with employment law obligations
- Support effective performance management
- Allow financial management and planning
- Enable equalities monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to, having regard to both data protection legislation and employment and trade union legislation which may be in force from time to time. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation, for example submission of school workforce census information to the Department for Education.
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way, for example accessing staff benefits such as childcare vouchers or cashless school catering payments
- We need to protect your or someone else's vital interests

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how consent may be withdrawn.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

Workforce data is important for school operations and the fulfilment of its functions. We collect personal information about you from you, from referees you nominate during the recruitment process, from line management and job-related activities whilst you are employed in the school and from external relevant bodies such as pre-employment checking and regulatory bodies, payroll and pension providers, and tax

authorities. While the majority of information we collect from or about you is routine and/or mandatory, there is some information that you can decline to provide.

Whenever we seek to collect information from you, we make it clear whether it is mandatory or optional.

How we store this data

We keep data securely for the time set out in our Records Management Policy which is available on request. Essentially, we keep information about you from the time you apply for a job with us, whilst you are employed at the school and for a limited time beyond your employment by the school, for practical reasons and in order to comply with our legal obligations.

We create and maintain a hard copy employment file for each staff member which is kept secure and maintained in our Human Resources department. We also store information electronically (for example on Arbor). Electronic data may be stored using cloud-based systems. The school engages external IT specialists to advise on and maintain the effectiveness and appropriate security of these systems.

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so. Subject to this, we may share personal information about you with:

- Harrow Council - We are required to share information about our workforce members with our local authority under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- Department for Education - We are required to share information about our school employees with the DfE under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.
- Trustees and Governors
- Educators and examining bodies
- Ofsted
- Payroll, taxation, pension, occupational health and HR providers and pre-employment check and regulatory agencies
- Suppliers and service providers
- Our auditors and insurers
- Professional bodies, advisers and consultants
- Police forces, courts, tribunals
- In certain situations, your family or representatives

Your rights regarding personal data

Under data protection legislation, you have the right to request access to information we hold about you. If you would like to make a request, please contact the Head teacher's PA, contact details below.

You also have the right to

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing

- Claim compensation for damages caused by a breach of the data protection regulations

Concerns and contacts

- To make a request to access your/your child's personal data, please contact the **Headteacher's PA,** (vfairweather@pinnerhighschool.org)

- If you have any queries, concerns or complaints, please contact our **Data Protection Officer, Data Protection Officer, Judicium Consulting Limited, 72 Canon Street, London, EC4N 6AE**, (dataservices@judicium.com)

- If you remain concerned, you can contact the **Information Commissioner's Office,** (https://ico.org.uk/concerns/)

Appendix 2: Processing Special Category Data (extract from the ICO website)

Special category data is broadly similar to the concept of sensitive personal data under the 1998 Act. The requirement to identify a specific condition for processing this type of data is also very similar.

One change is that the GDPR includes genetic data and some biometric data in the definition. Another is that it does not include personal data relating to criminal offences and convictions, as there are separate and specific safeguards for this type of data in Article 10. See the definitions section of this Guide for more detail on what counts as special category data.

The conditions for processing special category data under the GDPR in the UK are broadly similar to the Schedule 3 conditions under the 1998 Act for the processing of sensitive personal data. More detailed guidance on the new special category conditions in the Data Protection Act 2018 - and how they differ from existing Schedule 3 conditions - will follow in due course.

What's different about special category data?

You must still have a lawful basis for your processing under Article 6, in exactly the same way as for any other personal data. The difference is that you will also need to satisfy a specific condition under Article 9.

This is because special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

See the definitions section of this Guide for full details.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate.

What are the conditions for processing special category data?

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) 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 on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

You need to read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

- Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (g), (i) and (j).
- Schedule 1 Part 2 contains specific ‘substantial public interest’ conditions for Article 9(2)(h).
- In some cases you must also have an ‘appropriate policy document’ in place to rely on these conditions.

April 2026

Appendix 3: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

All staff and third-party data processors are contractually obligated to report any actual or potential data breach to the Head of Operations **without undue delay**.

The Head of Operations is responsible for the management of the breach scenario, including escalation of the incident to the external DPO if appropriate (depending on the scale and nature of the breach and the risk it creates to individuals' rights and freedoms.)

Responding to a data breach or potential data breach will include

- Assessment will decide if personal data has been subject to accidental or unlawful
- Appropriate and proportionate containment and mitigation measures.
- Evaluation of the **probability** or possibility of the risk occurring and the **severity** of the potential consequences for the affected individuals.
- Consideration of whether the breach must be reported to the ICO. This must be judged on a case-by-case basis and with advice from the DPO as appropriate. Relevant factors here would be whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through Loss of control over their data, discrimination, identify theft or fraud, financial loss, unauthorised reversal of pseudonymisation (for example, key-coding), damage to reputation, loss of confidentiality, any other significant economic or social disadvantage to the individual(s) concerned
- Documenting the above, including in the data breach log
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours.
- Consideration of whether it is appropriate to inform all individuals whose personal data has been breached. Again, this must be judged on a case-by-case basis and with advice from the DPO as appropriate.
- Where the incident involves **Special Category Data** (e.g., health, biometrics, or ethnicity), **Safeguarding records**, or **Criminal Offence data**, the school will treat the mitigation as a critical priority. We will act under the technical and legal instruction of our **Data Protection Officer (DPO)** and, where necessary, **Cyber Security specialists** or **Police authorities**, to execute a targeted recovery plan.
- Consideration of how similar breaches can be avoided in the future.

April 2026