Haydon School

Privacy Notice for Haydon Employees
(How we use your information)

Haydon School is a charitable company limited by guarantee (registration number 07557791) whose registered office is Haydon School Wiltshire Lane, Eastcote, Pinner, Middlesex, HA5 2LX.

This Privacy Notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Haydon School is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this Privacy Notice. This Privacy Notice should be read in conjunction with our GDPR Policy, Protection of Biometric Information Policy and Privacy Notice for Prospective Employees. It is important that you read this Privacy Notice, together with any other Privacy Notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

This Notice applies to current and former employees, workers and contractors. This Notice does not form part of any contract of employment or other type of contract to provide services. We may update this Notice at any time.

We have appointed a Data Protection Officer (DPO) to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your personal information, please email dpo@haydonschool.com.

Data protection principles
We comply with data protection law. This says that the personal information we hold about you must be:

- used lawfully, fairly and in a transparent way;
- collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
- relevant to the purposes we have told you about and limited only to those purposes;
- accurate and kept up to date;
- kept only as long as necessary for the purposes we have told you about;
- kept securely.

The type of information we hold about you
Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are also 'special categories' of more sensitive personal data which require a higher level of protection.

We will collect, store, and use the following categories of personal information about you:

- personal contact details such as name, title, addresses, telephone numbers, and personal email addresses;
- date of birth;
- gender;
- marital status and dependants;
- next of kin and emergency contact information;

- National Insurance number;
- bank account details, payroll records and tax status information;
- salary (including grade and salary band), annual leave, sick leave, special leave, maternity/paternity leave and pay, pension and benefits information;
- Teacher Reference Number;
- start and leave dates;
- copy of your passport or birth certificate and visa information (to check your entitlement to work in the UK);
- copy of your driving licence (if it is part of DBS documentation or to confirm your entitlement to drive the school minibus);
- recruitment information (please refer to our Privacy Notice for Prospective Employees for more information);
- employment records (including job titles, work history, working hours, working pattern (including any requests for flexible working), overtime, expenses or other payments claimed, training records and development needs, and professional memberships);
- health and wellbeing information declared by you, Occupational Health referrals, fit notes;
- compensation history;
- performance information;
- disciplinary and grievance information, including warnings issued to you;
- details of any access needs and reasonable adjustments;
- whistleblowing concerns raised by you, or to which you may be a party or witness;
- CCTV footage and other information obtained through electronic means such as swipecard records[1];
- information about your use of our information and communications systems and printing facilities;
- accident records if you have an accident at work;
- your responses to staff surveys if this data is not anonymised;
- photographs and video images.

'Special categories' of personal information

We may also collect, store and use the following 'special categories' of more sensitive personal information:

- information about your race or ethnicity, religious beliefs, sexual orientation and disability status for equal opportunities monitoring;
- trade union membership (for the purpose of the deduction of subscriptions directly from salary, to register the status of a protected employee and to comply with employment law obligations);
- information about your health, including any medical condition, health and sickness records;
- biometric data for cashless catering;
- information about your criminal record.

How we use particularly sensitive information

'Special categories' of particularly sensitive personal information require us to ensure higher levels of data protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- in limited circumstances, with your explicit written consent;
- where we need to carry out our legal obligations and in line with our GDPR Policy;
- where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our GDPR Policy;
- where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

[1] All of our ICT systems and the swipe access system for the entry and exit of our premises are auditable and can be monitored, though we don't do so routinely. We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our ICT systems and equipment. However, we reserve the right to log and monitor such use. Any targeted monitoring of staff will take place within the context of our disciplinary procedures.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Information about criminal convictions
We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our GDPR Policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions, for example, if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally required to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

Our obligations as an employer
We will use your particularly sensitive personal information in the following ways:

- we will use information relating to leaves of absence including the reasons for the leave, which may include sickness absence or family-related leave, sabbaticals, to comply with employment and other laws;
- we will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to comply with the Equality Act 2010, to monitor and manage sickness absence and to administer benefits;
- we will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting;
- we will use trade union membership information to pay trade union subscriptions, register the status of a protected employee and to comply with employment law obligations.

Do we need your consent?
We do not need your consent if we use your particularly sensitive information in accordance with our written policy where processing is necessary:

- to carry out our legal obligations or exercise specific rights in the field of employment law;
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- for reasons of substantial public interest, which shall be proportionate to the aim pursued and respect the essence of the right to data protection. The School will provide specific measures to safeguard the fundamental rights and the interests of the data subject.

In other circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract of employment with us that you agree to any request for consent from us.

How is your personal information collected

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, the Local Authority or other background check agencies (DBS and Atlantic Data). We will also collect additional personal information in the course of job-related activities

throughout the period of you working for us. We also get information about you from Occupational Health, pension provider, HMRC, and in some circumstances, from your Trade Union.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- where we need to perform the contract we have entered into with you and to provide you access to services required to your role;
- where we need to comply with a legal obligation;
- where it is needed in the public interest or for our official purposes;
- where it is in our legitimate interests, for example to manage our HR processes.

We may also use your personal information in the following situations:

- where we need to protect your interests (or someone else's interests);
- where we have your explicit consent.

Situations in which we will use your personal information

We need the information primarily to allow us to perform our contract with you, to enable us to comply with legal obligations and/or where it is needed in the public interest or for our official purposes as a school. The situations in which we will process your personal information are listed below:

- making a decision about your recruitment or appointment;
- determining the terms on which you work for us;
- checking you are legally entitled to work in the UK;
- to maintain a central record and to comply with our general safeguarding obligations;
- to provide information on our website about our employees;
- providing you access to services required to your role;
- paying you and, if you are an employee, deducting tax and National Insurance contributions;
- liaising with your pension provider;
- in order to operate as a school, which may involve us sharing certain information about our staff with our stakeholders or processing correspondence or other documents, audits or reports which contain your personal data;
- business management and planning, including accounting and auditing;
- conducting performance reviews, managing performance and determining performance requirements;
- establishing education, training and development requirements;
- making decisions about salary reviews and compensation;
- assessing qualifications for a particular job or task, including decisions about promotions;
- gathering evidence for possible grievance or disciplinary hearings;
- responding to complaints or investigations from stakeholders or our regulators;
- making decisions about your continued employment or engagement;
- making arrangements for the termination of our working relationship;
- providing references to prospective employers;
- dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- ascertaining your fitness to work (Occupational Health);
- managing sickness absence;
- complying with health and safety obligations;
- to prevent fraud;
- to monitor your use of our information and communication systems to ensure compliance with our IT policies;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- to conduct data analytics studies to review and better understand employee retention and attrition rates;
- in connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with an academy conversion;

- to maintain and promote equality in the workplace;
- to receive advice from external advisors and consultants;
- where appropriate, to disclose certain information in the school's accounts in accordance with the Accounts direction;
- in appropriate circumstances to liaise with regulatory bodies, such as the Teaching Regulation Agency, the Department for Education, the DBS and the Local Authority about your suitability to work in a school or in connection with other regulatory matters.

Additionally, **EPM**, our payroll and HR consultant, conducts the following on our behalf:

- checks the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working in specific positions;
- administers the contract we have entered into with you.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

In addition, the School uses CCTV cameras around the school site for security purposes and for the protection of staff and students. CCTV footage may be referred to during the course of disciplinary procedures (for staff or students) or investigate other issues. CCTV footage involving staff will only be processed to the extent that it is lawful to do so. Please see our CCTV Policy for more details.

Please note that all staff are issued with a pass that displays their name, job position and a photograph. Staff pass details (names and photographs) are held on a standalone machine in our Library managed by restricted number of staff (Network Manager, IT Technicians, Librarians). Information is uploaded to Paxton Net2 from SIMS and photographs – from our network drives. Should you lose your pass you will need to report in to the Librarian immediately. When you leave, your details will be deleted as soon as possible from this system.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers) or we may be unable to discharge our obligations which may be in the public interest or for official purposes.

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis that allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We do not envisage that any decisions will be taken about you by solely using automated means, however we will notify you in writing if this position changes.

Data sharing

We share your data with third parties, including third-party service providers and other organisations. In particular, we share your data with organisations including, but not limited to, the following:

- the Local Authority;
- the Department for Education;
- the Education & Skills Funding Agency;
- the Disclosure and Barring Service (DBS);
- the Teaching Regulation Agency;
- the Teachers' Pension Service;
- the Local Government Pension Scheme which is administered by Hillingdon Local Authority;

- LGfL;
- Atomwide;
- Google G Suite for Education;
- CPOMS, Safeguarding and Child Protection software;
- EPM, our external HR and payroll provider;
- our IT provider;
- HMRC;
- our auditors;
- an education recruitment agencies (agency and temporary staff);
- SatchelOne;
- SchoolCloud Systems, provider of our parents evenings booking system;
- Softlink, provider of our library management system;
- ParentPay, an online payment system;
- eduFOCUS, provider of our online software for the planning, approval and management of extra-curricular activities and our Accident Book;
- school external trips advisor;
- ESS SIMS;
- Npal (Inventry) – signing-in records;
- SAMpeople;
- PaperCut, print management software;
- Paxton Net2, our door entry/access control system;
- Wonde and Groupcall, 3rd party data extractors.

We also may share your personal information with:

- Public Health England;
- Occupational Health care provider;
- UCAS;
- Unifrog;
- school catering provider;
- Civica;
- the Joint Council for Qualifications;
- Buckinghamshire County Council (for SIMS support management);
- trip organisers;
- eDofE;
- the Police or other law enforcement agencies;
- our legal advisors;
- insurance providers (Risk Protection Arrangement);
- online learning platforms (Hegarty Maths, Sparx Maths, Kerboodle, BedRock, Activelearn, Focus on Sound, BandLab Technologies, Soundation, EZYEducation, Seneca, Quizlet, Pinpoint Learning, iDEA, Lexia, First News Ihub, ZigZag Education, GCSEPod);
- e4education, our website provider;
- NRS;
- PiXL.

Staff personal information (Emergency contact form) may be carried by school staff (Trip Leader) when on school educational visits.

Please be advised that we employ services of a confidential waste disposal company (Restore Datashred) for secure disposal of paper records.

Personal information in the public domain

Personal information classified as being in the 'public domain' refers to information which will be publicly available on our website and may be disclosed to third parties without recourse to the data subject. Depending on your role, the School may share your contact details (names, work phone number, staff

workplace email address and job title) on our website as well as share this information with parents/carers and our contractors/providers/processors. Where supplied and appropriate, we may share your academic qualifications and any additional information you have agreed to be placed in the public domain.

We require third parties to respect the security of your data and to treat it in accordance with the law. Some of the organisations referred to above are joint data controllers. This means we are all responsible to you for how we process your data. In the event that we share personal data about you with third parties, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data.

Why might we share your personal information with third parties?
We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you, where it is needed in the public interest or for official purposes, or where we have your consent.

Which third-party service providers process your personal information?
"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by the third-party service providers: payroll, HR, pension administration, benefits provision and administration, IT services, administration of trips and extra-curricular activities, electronic Accident Book among others.

Department for Education
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

We are required to share information about our students with the Department for Education (DfE) under regulation 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 as amended.

DfE data collection requirements
The following is information provided by the DfE concerning the reason it collects data about school employees: "The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005."

To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff by:

- conducting research or analysis;
- producing statistics; and/or
- providing information, advice or guidance.

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data .

To be granted access to school workforce information, organisations must comply with the DfE's strict terms and conditions covering the confidentiality and handling of the data, security arrangements and

retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

To contact the department: https://www.gov.uk/contact-dfe.

How secure is your information with third-party service providers?
All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

What about other third parties?
We regularly receive information requests under the DPA 2018 and the Freedom of Information Act (2000). We will consider whether to disclose staff information in response to these requests. We normally approach you for your permission prior to deciding whether to disclose information that is not within your reasonable expectations. However, we will normally disclose work-related information about staff in a public-facing role (Headteacher, Deputy Headteacher, Assistant Headteacher, Director of Finance and Operation, Lead Practitioners, DSL and Deputies SENCo, Year Leaders and their Deputies, Heads of Faculties, DPO). If you have any concerns about information being released or have a specific reason why your information cannot be disclosed, please email dpo@haydonschool.com.

Please be assured that we will only disclose your personal data if we are satisfied that it is reasonable to do so in all the circumstances. This means that we may refuse to disclose some or all of your personal data following receipt of such request.

If you leave, we may be asked by your new or prospective employer to provide a reference. For example, we may be asked to confirm the dates of your employment or your job role. If you are still employed by us at the time the request for a reference is received we will discuss this with you before providing reference.

Confidential references

Under the DPA 2018, an exemption has been made to allow references to be confidential, and therefore not accessible under a Subject Access Request. This exemption applies if you give or receive a confidential reference for the purposes of prospective or actual:

- education, training or employment of an individual;
- placement of an individual as a volunteer;
- appointment of an individual to office; or
- provision by an individual of any service.

It exempts the reference from the UK GDPR's provisions on:

- the right to be informed;
- the right of access; and
- all the principles, but only so far as they relate to the right to be informed and the right of access.

It is essential that you mark the reference as 'Confidential' for this to apply, and it would also be worth ensuring that the receiving organisation understood the new exemption, as otherwise they might share it. Please refrain from disclosing any sensitive information (please refer to our GDPR Policy for definition). If a reference does contain sensitive information please mark the reference as 'Confidential'.

Transferring information outside the EU

With cloud-based storage and some other services sometimes being supplied outside the UK, personal data can be sent to other jurisdictions. Where we transfer personal data to a country or territory outside the European Economic Area (EEA), we will do so in accordance with data protection law. If we do, you can expect a similar degree of protection in respect of your personal information. Our servers and storage systems are based in the EU or the EEA and we have ensured that appropriate safeguards are in place to protect your personal data.

We may sometimes transfer your personal data outside of the EU/EEA if, for example, we are arranging a school trip and we are booking transport, accommodation or activities. In these circumstances, we will obtain your consent for us to process your data in this way. When we transfer staff personal data overseas we ensure that we have appropriate safeguards in place.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available from the Network Manager and in our E-Safety and ICT Policy.

Third parties who are processing personal data on our behalf will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will we use your information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, insurance or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Records Management and Retention Policy, available from the DPO**,** dpo@haydonschool.com.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our Records Management and Retention Policy and applicable laws and regulations.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **request access** to your personal information (data subject access request). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it;
- **request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- **request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below);
- **object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes

you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes;
- **request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- **request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the DPO in writing.

The legal timescales for the school to respond to a Subject Access Request is one calendar month. As the school has limited staff resources outside of term time, we encourage staff to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays where possible. This will assist us in responding to your request as promptly as possible. For further information about how we handle Subject Access Requests, please see our GDPR Policy.

No fee usually required
You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is manifestly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you
We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent
In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the DPO, dpo@haydonschool.com. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Complaints
If you have a concern about the way we are collecting or using your personal data, we request that you raise it with us in the first instance. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. You can contact the Information Commissioners Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Last updated: March 2024 (v4)