



# **SOUTHEND HIGH SCHOOL FOR BOYS**

## **Privacy Notice for Staff and Applicants**

This Privacy Notice explains how we collect, store and use personal data about all school staff (including applicants for employment vacancies).

For the purposes of Data Protection legislation Southend High School for Boys is the Data Controller and responsible for the personal data collected about you.

Personal data is information about you from which you can be identified.

### **The categories of information (disclosed during the recruitment process or at any stage during employment) that we process include:**

- Personal information (such as name, address, contact details, employee or teacher number, national insurance number, address history and proof of identity)
- Bank details and other financial information
- Education, qualifications and professional achievements
- Special characteristic information (such as gender, age, ethnic group)
- Contract information (such as start date, hours worked, post, roles and salary information)
- Absence and health information (such as number of absences and reasons)
- Safeguarding checks (including DBS number)
- Relevant medical information (including physical and mental health and access requirements)
- Disciplinary related matters
- Information about you from a previous employer or an educational establishment which you have previously attended during the recruitment process
- Trade Union membership
- Job performance including career progression
- Car details
- CCTV imagery – *see separate policy*
- Photos (e.g. on school website, staff database, social media)
- Location data
- Telephone calls (retained for 30 days)
- For alumni – key employment data for archiving purposes (e.g. school history, tax or pension)

### **Why we collect and use workforce information**

Workforce data is essential for the school's operational use and the majority provided to us is mandatory, although some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you, at the point of collection, whether you are required to provide certain information to us or whether you have a choice.

We rely on having a legitimate reason to collect and use your personal information and to comply with our statutory obligations, and carry out tasks in the public interest.

We use workforce data to:

- a) Fulfil our duty of care towards our staff
- b) Provide employment services (e.g., payroll, pension payments and references)
- c) Facilitate safe recruitment
- d) Monitor absence and enable leave payments (e.g., sick pay, maternity leave, paternal leave)
- e) Enable ethnicity and disability monitoring
- f) Enable the development of a comprehensive picture of the workforce and how it is deployed
- g) Inform the development of recruitment and retention policies
- h) Inform financial audits of the school and allow better financial modelling and planning
- i) Inform national workforce policy monitoring and development

Under the Data Protection Act 2018, the legal basis we rely on for processing personal information is to fulfil contractual obligations and other legitimate interests. These are:

- **Consent:** an individual has given clear consent to process their personal data for a specific purpose
- **Contract:** necessary for a contract with an individual or specific steps required before entering into a contract
- **Legal obligation:** necessary to comply with the law
- **Public task:** necessary to perform tasks that the school is required to perform as part of their statutory function
- **Vital interests:** to keep children safe and protect your vital interests or someone else's
- **Legitimate interest:** necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data. The school relies on legitimate interest for most of the processing of your data. Specifically the school has a legitimate interest in:
  - looking after your welfare and development and the welfare and development of others;
  - safeguarding pupils;
  - staff recruitment;
  - management planning and forecasting, research and analysis, including that imposed or provided for by law (such as diversity or gender pay gap reporting);
  - financial transactions and reporting e.g., payroll, national insurance, pensions;
  - to give and receive information and references about past, current and prospective staff;
  - to monitor (as appropriate) use of the school's IT and communications systems, and for security purposes, CCTV and photo ID;
  - to carry out, or co-operate with, complaints, disciplinary or investigation processes;
  - to facilitate the efficient operation of the school;
  - to obtain appropriate professional advice and insurance for the school; and
  - ensure all relevant legal obligations of the school are complied with.

In addition, under Article 9 of the GDPR we will, on occasion, need to process special category personal data concerning health, racial or ethnic origin, political opinions, religion, trade union membership, sexual orientation or criminal record information, in accordance with rights or duties imposed by law. We rely upon reasons of substantial public interest (equality of opportunity and treatment, to protect the vital interest of any person where that person cannot give consent, legal claims or medical treatment).

## **Storing workforce information**

We hold data securely for the set amount of time shown in our data retention schedule and only for as long as we have a legitimate and lawful reason to retain it. Applicant information is stored for 12 months then securely destroyed. The legal recommendation for personnel files is 6 years after cessation of employment. However incident reports, safeguarding files and payroll/pension data are kept much longer, in accordance with specific legal requirement. For more information on our data retention schedule and how we keep your data safe, please contact the HR Manager.

Personal information that is no longer needed, or has become inaccurate or out of date, it is disposed of securely. We will shred or incinerate paper-based records and override electronic files. We may use an outside company to safely dispose of these records.

## **Who we share workforce information with**

We routinely share this information with:

- Southend High School for Boys' Governing Body
- Government authorities (e.g., the Department for Education (DfE), HMRC and local authority)
- Service providers (e.g., Juniper for HR services, Mazars for payroll, Essex Pension Fund, Teacher's Pension and Occupational Health)
- Disclosure and Barring Service (DBS) (e.g. during recruitment checks or a referral)
- Teachers Pensions
- Professional advisers (e.g., insurers, lawyers)
- NCTL (e.g., during recruitment checks or a referral)
- OFSTED
- UK Border Agency if employed under Tier 2 or Tier 5 to comply with our duties as a sponsor
- Sodexo if part of the child care salary sacrifice scheme. Details are provided only to the extent necessary for vouchers to be provided
- Education software providers
- Training providers
- Medical practitioners in the case of an emergency

We will share personal information with law enforcement or other authorities if required by law.

Personal data collected by us will, for the most part, remain within the school, and be processed by appropriate individuals in accordance with access protocols. Particularly strict access applies in the context of medical and safeguarding records.

The school is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as Local Authority Designated Officer (LADO) or police.

Some of the school's processing activity is carried out on its behalf by third parties, such as cloud storage providers. This is subject to contractual assurances that personal data is kept securely and in accordance with the school's specific direction.

## Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

### Our Local authority

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

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. 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 and sections 113 and 114 of the Education Act 2005.

All data is transferred securely and held by the DfE under a combination of software and hardware controls which meet the current [government security policy framework](#).

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. For more information please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>

## Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request to see your personal information, contact [enquiries@shsb.org.uk](mailto:enquiries@shsb.org.uk) to discuss making a Subject Access Request.

You also have the right to:

- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed

Depending on the reason for using your information, you may also be entitled to:

- have your information transferred electronically to yourself or to another organisation

- object to decisions being made that significantly affect you
- object to how we are using your information
- stop us using your information in certain ways

We will always seek to comply with your request however, we may be required to hold or use your information to comply with legal duties.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance either with the HR Manager ([HR@SHSB.org.uk](mailto:HR@SHSB.org.uk)) or our DPO ([dpo@shsb.org.uk](mailto:dpo@shsb.org.uk)).

Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>