KING EDWARD'S SCHOOL
POLICY DOCUMENT

Title: Staff Privacy Notice

Status	Approved
Approved by	Bursar
Current Author	Governance & Data Lead
Last Updated/Revised	September 2026
Application	Whole School
Responsibility	Bursar/ Governance & Data Lead

Contents

1.	Record of changes to this notice:	3
2.	How we collect your information	5
3.	The types of information we collect	5
4.	How we use your Information	6
5.	How we use Particularly Sensitive Information	8
6.	Sharing your information with others	10
7.	Security	10
8.	How long your information is kept	11
9.	Your rights	11
10.	Contact and complaints	11
11.	Contact and complaints	11

Specific Terms

King Edward's School, Bath (the School)
This privacy policy applies to all personal data processed by King Edward's School and its subsidiary companies, organisations, businesses and clubs. In this policy, these are all collectively called the "School". **King Edward's School is a charity** and our registered charity number is 1115875. **The King Edward's School, Bath 1552 Foundation,** charity number 1214031, works alongside the School on alumni engagement and fundraising activities and is considered part of the School for the purposes of this policy. **King Edward's School, Bath** and **The King Edward's School, Bath 1552 Foundation** jointly determine the purposes and means of processing certain personal data and therefore act as **joint controllers** under Article 26 UK GDPR **KES Bath Ventures Ltd,** a private limited company incorporated in England and Wales with company number 17165286, is a wholly-owned trading subsidiary of the School incorporated to undertake trading and commercial activities that support the charitable purposes of the School and is considered part of the School for the purposes of this policy. **King Edward's School, Bath** and **KES Bath Ventures Ltd** jointly determine the purposes and means of processing certain personal data and therefore act as **joint controllers** under Article 26 UK GDPR.

King Edward's 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.
Data Protection Officer:	Data Protection Education Ltd 41 High Street Royston, Hertfordshire, SG8 9AW Email: info@dataprotection.education.
Governance & Data Lead	Tracy Vaid Email: dataprotection@kesbath.com
Personal data	Any information relating to an identified or identifiable individual
Special category personal data and Criminal Offence data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership, Genetic and biometric data, Data concerning health, sex life or sexual orientation. Criminal offence data includes criminal activity, allegations, investigations and proceedings.

Record of changes to this notice:

June 2023	• Adaptation of template notice for KES specific use • Clarification of Data Protection Rights & Responsibilities
March 2026	• Inclusion of The King Edward's School, Bath 1552 Foundation, a subsidiary charity of King Edward's School, Bath, within this Privacy Notice.
Sept 2026	• Updates for new DPO • Changes to reflect KCSIE 2026 and DUAA

STAFF PRIVACY NOTICE

This notice is reviewed regularly and updated where necessary to reflect changes in law, regulatory guidance and the School's processing activities.

Copies of this notice will be available on the School website, the staff VLE and will be supplied to all the categories of staff identified below upon application or appointment as relevant.

This Staff Privacy Notice explains how the School collects, uses and shares (or "processes") your personal data during and after your work relationship with us, in accordance with the UK General Data Protection Regulation (UK GDPR) and your rights in relation to the personal data we hold.

This notice applies to staff at the School, including: employees, contractors, visiting music teachers and other peripatetic workers, casual workers, temporary workers, and volunteers who may be employed or engaged by the School to work for it in any capacity, as well as prospective applicants for roles.

Please note that, even if this Notice applies to you, references to "employment", “staff” etc. in this Notice are not intended to imply or confer any employment rights on you if you are a contractor, non-employed worker, or job applicant.

This Privacy Notice applies in addition to the School's other relevant terms and conditions and policies that may (depending on your role and status) apply to you, including

- any contract between the School and its staff, such as the terms and conditions of employment, staff code of conduct and any applicable staff handbook;
- the School’s CCTV and/or biometrics policy;
- the School's disciplinary, safeguarding, pastoral, anti-bullying, or health and safety policies, including as to how concerns, low-level concerns or incidents are reported or recorded (both by and about staff);
- the School’s data protection policy; and
- the School's IT policies, including its Acceptable Use policy and e-Safety policy.

Please note that any contract you may have with the School will be relevant to how the School processes your data, in accordance with any relevant rights or obligations under that contract. However, this Staff Privacy Notice is the primary document by which we notify you about the use of your personal data by the School.

This Staff Privacy Notice also applies alongside any other information the School may provide about particular uses of personal data, for example when collecting data via an online or paper form.

How we collect your information

We may collect your personal data in a number of ways, for example:

- from the information you provide to us before making a job application, for example when you come for an interview;
- when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, or when you complete a self-declaration, etc.; and
- from third parties, for example the Disclosure and Barring Service (DBS) and referees (including your previous or current employers or School), or from third party websites (as part of online suitability checks for shortlisted candidates) or (if you are a contractor or a substitute) your own employer or agent, in order to verify details about you and/or your application to work for us.

More generally, during the course of your employment with us, as a member of staff, we will collect data from or about you, including:

- when you provide or update your contact details;
- when you or another member of staff completes paperwork regarding your performance, objectives or professional development;
- in the course of fulfilling your employment (or equivalent) duties more generally, including by filling out reports, note taking, or sending emails on School systems;
- in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below;
- by completing staff self-declaration forms.

The types of information we collect

We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant):

- **contact and communications information, including:**
    - your contact details (including email address(es), telephone numbers and postal address(es);
    - contact details (through various means, as above) for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this Privacy Notice;
    - records of communications and interactions we have had with you;
- **biographical, educational and social information, including:**
    - your name, title, gender, nationality and date of birth;
    - your image and likeness, including as captured in photographs taken for work purposes;
    - details of your education and references from your institutions of study;
    - lifestyle information and social circumstances;
    - your interests and extra-curricular activities;
    - information in the public domain, including information you may have posted to social media, where relevant to your role (e.g. as part of pre-employment screening);

- **financial information, including:**
    - your bank account number(s), name(s) and sort code(s) (used for paying your salary or invoices and processing other payments);
    - your tax status (including residence status);
    - information related to pensions, national insurance, or employee benefit schemes;
- **work related information, including:**
    - details of your work history and references from your previous employer(s);
    - your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for the School;
    - details of your professional activities and interests;
    - your involvement with and membership of sector bodies and professional associations;
    - information about your employment and professional life after leaving the School, where relevant (for example, where you have asked us to keep in touch with you);
    - nationality and other immigration status information (i.e. about your entitlement to work in the UK), including copies of passport information (if applicable);
- **and any other information relevant to your employment or other engagement to work for the School.**

Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data, and information about criminal convictions and offences, including:

- information revealing your racial or ethnic origin;
- trade union membership, where applicable;
- information concerning your health and medical conditions (for example, where required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment);
- biometric information, for example where necessary for School security systems;
- information concerning your sexual life or orientation (for example, in the course of investigating complaints made by you or others, for example concerning discrimination); and
- information about certain criminal convictions (for example, where this is necessary for due diligence purposes, whether by self-declaration or otherwise, or for compliance with our legal and regulatory obligations).

However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for the School.

How we use your Information

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

- Where we need to perform the contract we have entered into with you;
- Where we need to comply with a legal obligation (such as health and safety legislation, under statutory codes of practice and employment protection legislation);

- Where it is necessary for our legitimate interests (or those of a third party) and your interests, rights and freedoms do not override those interests;
- When you have provided us with consent to process your personal data.

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

The situations in which we will process your personal information are listed below:

- To determine recruitment and selection decisions on prospective employees;
- In order to carry out effective performance of the employees contract of employment and to maintain employment records;
- To comply with regulatory requirements and good employment practice;
- To carry out vetting and screening of applicants and current staff in accordance with regulatory and legislative requirements;
- Enable the development of a comprehensive picture of the workforce and how it is deployed and managed;
- To enable management and planning of the workforce, including accounting and auditing;
- Personnel management including retention, sickness and attendance;
- Performance reviews, managing performance and determining performance requirements;
- In order to manage internal policy and procedure;
- Human resources administration including pensions, payroll and benefits and employee reward schemes;
- To determine qualifications for a particular job or task, including decisions about promotions;
- Evidence for possible disciplinary or grievance processes;
- Complying with legal obligations;
- To monitor and manage staff access to our systems and facilities to protect the personal data of our employees and for the purposes of safeguarding via operating filtering, monitoring and online-safety systems;
- To safeguard children and fulfil the School's safeguarding obligations, including recording and investigating safeguarding concerns, allegations and low-level concerns; assessing suitability to work with children; making statutory or regulatory referrals; and cooperating with safeguarding partners and regulators where required.
- To monitor and protect the security of our network and information, including
    - preventing unauthorised access to our computer network and communications systems
    - preventing malicious software distribution;
    - protecting networks, accounts, devices and premises;
    - detecting unauthorised access, misuse, cyber-security threats and safeguarding risks
- Education, training and development activities;
- To monitor compliance with equal opportunities legislation;
- To answer questions from insurers in respect of any insurance policies which relate to you;
- Determinations about continued employment or engagement;
- Arrangements for the termination of the working relationship;
- Dealing with post-termination arrangements;
- Health and safety obligations;
- Prevention and detection of fraud or other criminal offences; and
- To defend the School in respect of any investigation or court proceedings and to comply with any court or tribunal order for disclosure.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your 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, or we may be prevented from complying with our legal obligations.

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.

Use of AI-assisted and automated systems

The School may use digital systems that include automated or artificial intelligence-assisted functionality for administrative, security, safeguarding, recruitment, transcription, accessibility and operational purposes. The School will only use such functionality where it has identified an appropriate lawful basis, assessed the privacy risks, applied data minimisation and security controls, and put appropriate contractual arrangements in place with relevant providers.

AI-assisted outputs will be subject to appropriate human oversight where they may affect an individual. The School does not make solely automated decisions about staff which produce legal or similarly significant effects. Further information about a particular system or processing activity may be provided at the point of collection or on request.

Please note that many of these digital and AI-supported tools include integrated filtering and monitoring features used to maintain cyber security, service resilience, and safeguarding obligations. Further information on the use of AI tools can be found in our AI policy.

How we use Particularly Sensitive Information

Special category personal data

The School processes special category data only where an Article 6 lawful basis and an applicable Article 9 condition are identified. Depending on the circumstances, this may include employment and social protection obligations, substantial public interest, occupational health, legal claims, vital interests or explicit consent.

Such information may be processed for purposes including sickness and absence management, occupational health, workplace adjustments, safeguarding, equality monitoring, employment benefits and compliance with employment and other legal obligations.

Criminal Convictions and Safeguarding-Related Information

The School may collect and process information relating to criminal convictions, criminal offences, allegations, safeguarding concerns, disciplinary findings, barring decisions, regulatory investigations and other relevant incidents where this is necessary to fulfil its safeguarding, employment, legal, regulatory and insurance obligations.

This may include information provided by employees, workers, volunteers, governors, contractors and applicants through recruitment processes, self-declaration forms, safeguarding questionnaires, incident reports, disclosure forms and Disclosure and Barring Service (DBS) checks.

In particular, the School may require individuals to disclose:

- unspent criminal convictions and cautions;
- information relevant to enhanced DBS checking and barring status;

- safeguarding allegations, investigations or findings;
- professional misconduct findings or regulatory sanctions;
- incidents that may affect suitability to work with children or vulnerable individuals; and
- matters which may be relevant to the School's insurance, health and safety, safeguarding or legal obligations.

The School will process such information only where:

- a lawful basis under Article 6 UK GDPR applies;
- the processing is authorised by UK data protection legislation;
- a relevant condition under Schedule 1 of the Data Protection Act 2018 applies where required, including safeguarding of children and individuals at risk, preventing or detecting unlawful acts, or exercising employment rights and obligations; and
- appropriate confidentiality, security, retention and access controls are in place.
- Access to criminal offence and safeguarding-related information is strictly limited to those with a legitimate need to know, such as safeguarding leads, senior leaders, human resources staff, legal advisers, insurers and regulatory authorities where required by law.

Insurance and Risk Management

The School may collect and disclose information concerning criminal convictions, safeguarding incidents, disciplinary matters or other relevant risk information where necessary to obtain, maintain or administer insurance cover, manage risk, investigate incidents, defend legal claims or comply with insurer requirements. Such disclosures will be limited to information that is relevant and proportionate for the purpose concerned.

Sharing your information with others

For the purposes referred to in this privacy notice and relying on the grounds for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases special category or criminal data) to a variety of recipients including:

- other employees, agents and contractors (eg third parties processing data on our behalf as part of administering payroll services, the provision of benefits including pensions, IT etc. – although this is not sharing your data in a legal sense, as these are considered data processors on our behalf);
- DBS and other government authorities (e.g. HMRC, DfE, CAFCASS, police, Home Office, a relevant public health / NHS body and / or local authority) and/or appropriate regulatory bodies (e.g. the Teaching Regulation Agency, the Independent Schools Inspectorate, the Charity Commission etc.);
- external auditors or inspectors;
- our advisers where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, or other external consultants;
- when the School is legally required to do so (by a court order, government body, law enforcement agency or other authority of competent jurisdiction), for example HM Revenue and Customs or police.

Information will be provided to those agencies securely or anonymised where possible.

The recipient of the information will be bound by confidentiality obligations, we require them to respect the security of your data and to treat it in accordance with the law.

We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations. References given or received in confidence may not be accessible under your UK GDPR rights.

International transfers
Some of the School's service providers may process personal data outside the United Kingdom. Where this constitutes a restricted transfer, the School will ensure that an appropriate transfer mechanism is in place in accordance with UK data protection law.

Security

We have put in place measures to protect the security of your information (i.e. against it being accidentally lost, used or accessed in an unauthorised way). 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.

Please contact the Governance & Data Lead if you require further details of our security procedures.

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.

How long your information is kept

Personal data relating to unsuccessful job applicants is deleted within 12 months except where we have notified you we intend to keep it for longer (and you have not objected).

How long we keep your information
The School retains workforce information only for as long as necessary for the purposes for which it was collected, including to meet legal, regulatory, safeguarding, tax, pension, insurance and employment obligations and to establish, exercise or defend legal claims. Specific retention periods are set out in the School's Records Retention Schedule and relevant processing records. Different categories of workforce information may therefore be retained for different periods.

Your rights

You have the following rights:

- to obtain access to, and copies of, the personal data that we hold about you;
- to require us to correct the personal data we hold about you if it is incorrect;
- to require us (in certain circumstances) to erase your personal data;
- to request that we restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);
- to receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller;
- to object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights.

If you want to exercise any of the above rights, please contact the Governance & Data Lead in writing via dataprotection@kesbath.com

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). You can find out more about your rights under applicable data protection legislation from the Information Commissioner's Office website available at www.ico.org.uk.

Contact and complaints

If you have any queries about this privacy notice or how we process your personal data, or if you wish to exercise any of your rights under applicable law, you should contact the Governance & Data Lead.

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 Governance & Data Lead. 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.

We hope that the Governance & Data Lead can resolve any query you raise about our use of your information in the first instance. See contact details on Page1.

We have appointed a Data Protection Officer (DPO) to oversee compliance with data protection and this privacy notice. If you have any questions about how we handle your personal information which cannot be resolved by the Governance & Data Lead, then you can contact the DPO – see contact details on page 1.

Making a data protection complaint

You may make a data protection complaint to the School by contacting the Governance & Data Lead using the details in this notice. We will acknowledge receipt within 30 days. We will take appropriate steps to investigate and respond to the complaint without undue delay, keep you informed of progress and notify you of the outcome.If you remain dissatisfied, you may contact the Data Protection Officer or complain to the Information Commissioner's Office.

Further details on how to do so can be found at https://ico.org.uk/make-a-complaint/

September 2026

Summary of Processing of Personal Data

Activity	Main Lawful Basis	Typical Data
Recruitment, selection and appointment	Contract (steps before entering into a contract) / Legitimate Interests	Application details, contact information, employment history, qualifications, references and interview/selection information
Safer recruitment, vetting and suitability checks	Legal Obligation / Legitimate Interests	Identity, right-to-work information, references, self-declarations, DBS and criminal offence information, and relevant publicly available information
Employment, contracts, payroll, pensions and benefits	Contract / Legal Obligation	Personal and contact details, employment records, salary, bank details, National Insurance, tax, pension and benefits information
Attendance, sickness, wellbeing and workplace adjustments	Contract / Legal Obligation / Legitimate Interests	Attendance and absence records, health information, sickness records, occupational health and workplace-adjustment information
Performance, training and professional development	Contract / Legitimate Interests	Performance and appraisal records, objectives, qualifications, training and professional development information
Disciplinary, grievance, complaints and internal procedures	Contract / Legitimate Interests / Legal Obligation	Employment records, correspondence, allegations, witness information, investigation records and outcomes
Safeguarding and child protection	Legal Obligation / Legitimate Interests	Safeguarding concerns, allegations, low-level concerns, suitability information, referrals and relevant criminal offence information
School premises, systems, accounts and network security	Legitimate Interests / Legal Obligation	Account and authentication information, access records, system and network activity, filtering and monitoring information and CCTV
Employment, equality, health and safety, regulatory and insurance obligations	Legal Obligation / Legitimate Interests	Employment information, equality information, health and safety records, accident/incident information, insurance and regulatory records
Legal claims and ending the working relationship	Legal Obligation / Legitimate Interests / Contract	Employment and termination records, correspondence, disciplinary or grievance information, legal and regulatory records

Lawful Basis for Processing Personal Data

The lawful basis we rely upon depends on the purpose and circumstances of the processing, and more than one lawful basis may apply. Where we process special category personal data, we will identify both an Article 6 lawful basis and an appropriate Article 9 UK GDPR condition. Where we process criminal offence data, we will ensure that the additional requirements of data protection law are met.

The School maintains a detailed Record of Processing Activities (RoPA) and, where required, supporting Data Protection Impact Assessments (DPIAs).