



KEW COLLEGE

Privacy Notice - Employee

See also the School's policies as follows:

CCTV Policy, Complaints Policy and Procedure, Data Protection Policy, Online Safety Policy, Record Retention Policy, Record Management Guidelines, Recruitment and Selection Policy, Safeguarding and Child Protection Policy

Definitions or abbreviations used in this Privacy Notice

Employee: Includes those who work on a permanent and non-permanent basis, including temporary and contract workers, governors, 3rd party providers, independent contractors, consultants, professional advisors, trainers and secondees.

DSL: Deputy Safeguarding Lead

LADO: Local Authority Designated Officer

Sensitive personal data ('special categories of personal data' under the General Data Protection Regulation) includes any information that reveals your racial or ethnic origin, religious, political or philosophical beliefs, genetic data, biometric data for the purposes of unique identification, trade union membership, or information about your health/sex life.

1. WHAT THIS PRIVACY NOTICE IS FOR

This Privacy Notice is intended to provide information about how the School will use (or "process") personal data about its staff and job applicants (referred to in this Notice as "you") and the rights you have in connection with this personal data.

This information is provided because Data Protection Law gives individuals rights to understand how their data is used.

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

This Privacy Notice also applies in addition to the School's other relevant terms and conditions and policies, including any contract between the School and its staff.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should also be aware of and comply with this Privacy Notice and the School's Data Protection Policy, which also provides further information about how your personal data will be used.

The School will update this Privacy Notice periodically to reflect any necessary changes in our privacy practices. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable. We encourage you to check this notice periodically to be aware of the most recent version.

2. RESPONSIBILITY FOR DATA PROTECTION

- The School has appointed two Privacy Officers, one for systems and IT related matters, the other for operational matters
- The Privacy Officers, together with the Head of Finance & Operations and HR Manager will deal with all your requests and enquiries concerning the School's uses of your personal data (see section on 'Your Rights' below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law. (See below for contact details)

3. WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

In order to carry out its ordinary duties to staff, the School needs to process a wide range of personal data about individuals (including current, past and prospective staff) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff.

Other uses of personal data will be made in accordance with the School's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The School expects that the following uses will fall within that category of its (or its community's) "**legitimate interests**":

- For the purposes of staff admission (and to confirm the identity of prospective staff)
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as tax, diversity or gender pay gap analysis)
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate
- To safeguard pupils' welfare
- To monitor (as appropriate) use of the School's IT and communications
- To make use of photographic images of employees in School publications, on the School website and (where appropriate) on the School's social media channels
- For security purposes, CCTV is in operation in accordance with the School's CCTV Policy
- To carry out or cooperate with any School or external complaints, disciplinary or investigation process
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School

In addition the School will, on occasion, need to process **special category personal data** (concerning protected characteristics or health or **criminal offence data** (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons will include:

- To provide appropriate medical care where necessary, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, and cooperation with police or social services, for insurance purposes or to caterers or organisers of School trips who need to be made aware of dietary or medical needs
- In connection with employment of its staff, for example DBS checks, welfare, union membership or pension plans
- As part of any School or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health or safeguarding elements
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care

4. TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example:

- Identification data: names, addresses, gender, photograph, date of birth, telephone numbers, e-mail addresses
- Contact details: home and business address, telephone/email addresses, emergency contact details
- Employment details: job title/position, employment contract, performance and disciplinary records, grievance procedures, sickness/holiday records
- Background information: academic/professional qualifications, education, CV, criminal records data (for vetting purposes, where permissible and in accordance with applicable law)
- Spouse & dependents information, marital status
- Financial information: banking details, tax information, withholdings, salary, benefits, expenses, allowances
- IT information – information required to provide access to our IT systems and networks such as IP addresses, log files and login information
- The type of personal information we process is limited to that needed to manage your specific work assignment
- References relating to previous roles and employment conduct may be undertaken prior to commencement of employment. We will only gather references from referees provided to us by the employee, or prospective employee
- correspondence with and concerning staff
- images of employees engaging in School activities, and images captured by the School's CCTV system (in accordance with the School's policy on Taking, Storing and Using images of Pupils)

The School tries not to collect or process any sensitive personal information about you, unless authorised by law or where necessary to comply with applicable laws. In some circumstances,

we may need to collect some sensitive personal information for legitimate employment-related purposes: for example:

- data relating to your racial/ethnic origin, gender and disabilities for the purposes of:
 - equal opportunities monitoring
 - to comply with anti-discrimination laws
 - for government reporting obligations
- data relating to your physical or mental health to:
 - provide work-related accommodations
 - health and insurance benefits to you and your dependents
 - to manage absences from work

5. HOW THE SCHOOL COLLECTS DATA

Generally, the School receives personal data from the individual directly. This may be via a form, through staff inputting data directly into Schoolbase, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data will be supplied by third parties (for example another School, or other professionals or authorities working with that individual); or collected from publicly available resources.

6. PURPOSES FOR PROCESSING PERSONAL DATA

6.1 Recruitment

If you are applying for a role with us then we collect and use personal data for recruitment purposes (in particular, to determine your suitability for a specific role) and for the purposes of managing the hiring process and communicating with you about it.

If you are accepted for a role with us, the data collected during the recruitment process will form part of your ongoing employee record.

For more information, please see the Recruitment and Selection Policy.

6.2 Employment

We collect and process personal data relating to our employees to meet our obligations under the employment contract and to comply with our legal obligations. We take the security of your data seriously and are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

Once you become an employee, we collect and use this personal information for managing our employment or working relationship with you – for example, your employment records and contract information (so we can manage our employment relationship with you), your bank account and salary details (so we can pay you), and details of your spouse and dependents (for emergency contact and benefits purposes).

Where we process special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that we use for these purposes is anonymised or is only collected with the express consent of employees or prospective employees, which can be withdrawn at any time.

We have policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed without authorisation and only accessed or used for specific legal purposes.

You have some obligations under your employment contract to provide the organisation with data. You may also have to provide the organisation with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide this data may mean that you are unable to exercise your statutory rights.

We process our employees' personal information through **Schoolbase** (our Management Information System), **Sign in Central Record** provided by Sign in solutions, **Smart Clinic** (our occupational health providers) and **Greenpay** (payroll agent). **Schoolbase** is provided by Furlong Solutions. These three providers are based in the United Kingdom and have provided contractual assurances that personal data is kept securely.

6.3 Legitimate business purposes

We may also collect and use personal information when it is necessary for other legitimate purposes, such as to help us conduct our business more effectively and efficiently – for example, for general IT security management, accounting purposes or financial planning. We may also process your personal information to investigate violations of law or breaches of our own internal policies.

The IT Department records and monitors usage of our IT equipment, user activity, email and Internet usage as deemed necessary. The IT Department will observe the strictest confidentiality when undertaking these activities. They will make their report directly to the DSL and/or Head who will determine the actions that may need to be taken in any particular case.

Our sites are protected by circuit television (CCTV) systems as deemed necessary (see CCTV Policy). Any information obtained from systems will be used with strict adherence to the GDPR. Information will be used for the prevention and detection of crime and to ensure compliance with our policies and procedures and our legal obligations. This may include using recorded images as evidence in disciplinary proceedings.

6.4 Legal purposes

We may use your personal data where we consider it necessary for complying with laws and regulations, including collecting and disclosing employee personal information as required by law (e.g. for tax, health and safety, anti-discrimination laws), under judicial authorisation, or to exercise or defend our legal rights.

7. WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

Personal data collected by the School will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Personal data will only be processed by third parties who have a legitimate purpose for accessing it. Whenever the School permits a third party to access personal information, we implement appropriate measures to ensure the data is used in a manner consistent with this Notice and that the security and confidentiality of the data is maintained.

7.1 Transfers to third-party service providers

The School will need to share some personal data with third party advisers such as lawyers, insurers, payroll support, tax advisers, health and safety support, PR advisers and accountants.

In addition, in accordance with Data Protection Law, some of the School's processing activity is carried out on its behalf by other third parties, such as IT systems, web developers or cloud storage providers. This is subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

We may need to transfer personal data to countries outside of the United Kingdom. When we export personal data to a different country, we will take steps to ensure that such data exports comply with applicable UK laws. For example, if we transfer personal data outside the European Economic Area (EEA), such as to the United States, we will implement an appropriate data export solution such as entering into contracts with the data importer that contain EU model clauses or taking other measures to provide an adequate level of data protection.

Other than those listed below, all our external providers store the employee data that we provide them in premises within the European Economic Area (EEA). For the external providers that have data hosted or processed in locations outside of the EEA, the School has reviewed the data stored, and considers that the risk of continuing to use each provider is acceptable.

Provider	Reason for Use	Data stored outside of the EEA
Book Creator for iPad	Teaching – e-book creation	USA – teacher log in data, pupil log in, pupil name.
Boxall Profile	Learning enrichment	USA – School payment details USA – teacher customer support
Canva for Education	Photo and video editor	USA – pupil first name
CoSpaces Edu	3D creations and coding	Outside EEA - pupil log in, pupil name
Doodle Spell	Teaching - spelling	Outside EEA – first name and DOB
iHasco	Staff training	USA – School payment details USA – customer support
InVentry	Visitor management	USA – School customer support
Minecraft Education	Teaching resource	Outside EEA – pupil log in, pupil name
Ozobot	Teaching - Coding robots	Outside EEA – parent email
Padlet	Teaching – virtual bulletin boards	Outside EEA – teacher log in, pupil first names
ScratchJr	Teaching – coding	Outside EEA – pupil name. but used without sign in, so no data stored

Seesaw	Teaching – classroom sharing	USA – teacher log in, pupil first names and photos
Twinkl	Teaching resource	USA – teacher log in

7.2 Transfers to other third parties

We may also disclose personal data to third parties on other lawful grounds, including:

- To comply with our legal obligations, including where necessary to abide by law, regulation or contract, or to respond to a court order, administrative or judicial process
- In response to lawful requests by public authorities (including for national security or law enforcement purposes)
- As necessary to establish, exercise or defend against potential, threatened or actual litigation
- Where necessary to protect the vital interests of our employees or another person
- In connection with the sale, assignment or other transfer of all or part of our business
- With your freely given and explicit consent

8. HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff personnel files is up to 7 years following departure from the School. This allows the School to respond to employment or work-related inquiries or to deal with any legal matters (e.g. judicial or disciplinary actions), document the proper termination of your employment or work relationship (e.g. to tax authorities), or to provide you with ongoing pensions or other benefits. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements.

If you have any specific queries about how our retention policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Head of Finance & Operations or HR Manager. However, please bear in mind that the School will often have lawful and necessary reasons to hold on to some personal data even following such a request.

A limited and reasonable amount of information will be kept for archiving purposes.

Kew College has a Record Management Guideline to establish guidelines and procedures for identifying, retaining, protecting, storing and disposing of records and documents (“Records”) belonging to the School. Protection of Records is a key element of corporate security and the responsibility of all staff. Good Record Retention and appropriate disposal of Records are essential components of the School’s commitment to integrity, the effective overall management of the School, and compliance with regulatory and legal obligations.

9. YOUR RIGHTS

9.1. Rights of access, etc.

Individuals have various rights under Data Protection Law to access and understand personal data about them held by the School, and in some cases ask for it to be erased or amended or have it transferred to others, or for the School to stop processing it – but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the Head of Finance & Operations.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is one month in the case of requests for access to information).

The School will be better able to respond quickly to smaller, targeted requests for information. If the request for information is manifestly excessive or similar to previous requests, the School may ask you to reconsider, or require a proportionate fee (but only where Data Protection Law allows it).

9.2. Requests that cannot be fulfilled

You should be aware that the right of access is limited to your own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals, or information which is subject to legal privilege (for example legal advice given to or sought by the School, or documents prepared in connection with a legal action).

With regard to the "right to be forgotten", there may on occasion be compelling reasons to refuse specific requests to amend, delete or stop processing your personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this Privacy Notice. All such requests will be considered on their own merits.

Under sch.2 to the Data Protection Act 2018 (which supplements the GDPR) employers are exempt from having to provide access to a confidential employment reference to an employee or former employee.

9.3. Consent

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time. An example where we rely on consent is certain types of use of images. Please be aware however that the School may not be relying on consent but have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment contract).

10. DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals should ensure that they update Schoolbase and notify the HR Manager of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law). See above for details of why the School may need to process data, and who should be contacted if the individual disagrees with such processing. The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to School systems.

All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

11. QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the Bursar or HR Manager using the contact details below.

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the School complaints procedure as outlined in the Complaints Policy and should also notify the Head. The individual can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator.

12 CONTACT DETAILS

Head of Finance & Operations: Jim Francis (email: jfrancis@kewcollegeprep.com or TEL: 020 8940 2039)

HR Manager: Nicola Harding (email: nharding@kewcollegeprep.com TEL: 020 8940 2039)

Or write to the above at:

Kew College Prep
24-26 Cumberland Road
Kew
Surrey TW9 3HQ

Approved by:	Updated by:
Name: Jane Bond	Name: Kim El-baz/Nicola Harding
Title: Head	Title: Compliance Officer/HR Manager
Date: 29 Jan 2025	Date: 29 Jan 2025