



# Kingswood House School

## Data Protection Policy

**This policy is reviewed annually to ensure its compliance with the latest regulations.**

Created by	<b>Sally Witts</b>	Date <b>September 2022</b>
Review by	<b>Campbell McKelvie (Compliance)</b>	<b>on 20 October 2023</b>
Next review date	<b>20 October 2024</b>	

### **Data Protection forms included in this policy:**

- *GDPR Parent Consent form (Appendix A)*
- *GDPR Pupil Consent form – Year 8+ (Appendix B)*
- *Open Morning Questionnaire (Appendix C)*

### **Background**

Data protection is an important legal compliance issue for Kingswood House School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the School's Privacy Notices. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School is the controller of pupils' personal information.

As a data controller, we are responsible for safeguarding the use of personal data.

- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or personal data)**: any information relating to a living individual (a data subject), including name, identification number, location or online identifier such as an email address. Note that personal information created in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings) is still personal data and regulated by data protection laws, including the GDPR. Note also that it includes expressions of opinion about the individual or any indication of someone's intentions towards that individual.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

### **Application of this policy**

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or Governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers - this may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers - each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

## Person responsible for Data Protection at the School

The School has appointed Campbell McKelvie (Compliance Officer) as the Data Protection Co-ordinator, who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Co-ordinator at [compliance@kingswoodhouse.org](mailto:compliance@kingswoodhouse.org).

## The Principles

The GDPR sets out six principles relating to the processing of personal data, which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The GDPR's 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data; and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

## Lawful grounds for data processing

Under the GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as GDPR requires.

Other lawful grounds include:

1. compliance with a legal obligation, including in connection with employment, engagement of services and diversity;

2. contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
3. a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

## **Headline responsibilities of all staff**

### **Record keeping**

It is important that personal data held by the School is accurate, fair and adequate. You are required to inform the School if you believe that *your* personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others – in particular colleagues, pupils and their parents – is accurate, professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.**

### **Data handling**

All staff have a responsibility to handle the personal data, which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the Staff Handbook and all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Child Protection and Safeguarding Policy, E-Safety Policy, Taking, Storing and Using Images of Children Policy, Bring Your Own Device to Work Policy and CCTV Policy. This list is not exhausted.

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

### **Avoiding, mitigating and reporting data breaches**

One of the key new obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those, which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. In any event, the School must keep a record of any personal data breaches, regardless of whether we need to

notify the ICO. If staff become aware of a personal data breach they must notify Campbell McKelvie (Compliance Officer). If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

### **Care and data security**

More generally, we require all School staff to remain conscious of the data protection principles, to attend any training we require them to, and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to Campbell McKelvie (Compliance Officer), and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

### **Rights of Individuals**

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a data controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell Campbell McKelvie (Compliance Officer) as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of our particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell Campbell McKelvie (Compliance Officer), as soon as possible.

### **Data Security: online and digital**

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. As such:

- No member of staff is permitted to remove personal data from the School premises in paper or electronic form and wherever stored, without prior consent of the Head, Bursar or Compliance Officer.
- Where a worker is permitted to take data offsite it will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

### **Summary**

It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.

## Personal Data Consent Form Parent/Carer

Dear Parent/Carer

Your child's personal data comes in different forms. It can be their photo in the School magazine or prospectus, or a video of their School trip or match fixture. The School makes various uses of this data and some of these are necessary for administration purposes and their safety, such as storing medical details and CCTV images. We would also like to celebrate your child's time at School in our publications such as the newsletter, in print and digitally, on our website or Social Media sites.

To comply with the General Data Protection Regulation 2018 (GDPR), we need to have your permission to store or use personal data whilst your child is a pupil at Kingswood House and after they have left.

If you wish to discuss further how the School uses this personal data, please contact Mr Walid Chaudhry, Compliance Officer or read the School Privacy Notice on our website.

Please indicate below if you understand the above and are happy to consent to your child's data being used in this way. You may withdraw your consent at any time in the future by letting the School Office know in writing. Once your child has reached the age of consent (year 8+), we will be seeking their permission as well.

Please be aware that it may only be possible to remove online images and that we cannot change printed materials once published.

Pupil's Name..... Current Form.....

<b>Sensitive and Personal Data</b>	<b>Tick</b> ✓
I am happy for the School to store/hold my child's personal data including sensitive and personal information as detailed above.	

<b>Use of photos and videos</b>	<b>Tick</b> ✓
I am happy for the School to take, store or use photos and videos of my child as detailed above.	

I understand that it is my responsibility to inform the School in writing if I decide to withdraw my consent.

Parent/Carer's Name (Please print).....

Sign.....

Date.....

**Personal Data Consent Form  
Year 8+**

Dear Pupil

Your personal data comes in different forms. It can be your photo in the School magazine or prospectus, or a video of your School trip or match fixture. The School makes various uses of your data and some of these are necessary for administration purposes and your safety, such as storing your medical details and CCTV images. We would also like to celebrate your time at School in our publications such as the newsletter, in print and digitally, on our website or Social Media sites.

To comply with the General Data Protection Regulation 2018 (GDPR), we need to have your permission to store or use your personal data whilst you are a pupil at Kingswood House and after you have left.

If you wish to discuss further how the School uses your personal data, please ask your form teacher or read the School Privacy Notice on our website.

Please indicate below if you understand the above and are happy to consent to your data being used in this way. You may withdraw your consent at any time in the future by letting the School Office know in writing.

Please be aware that it may only be possible to remove online images and that we cannot change printed materials once published.

Pupil's Name..... Current Form.....

<b>Sensitive and Personal Data</b>	<b>Tick</b> √
I am happy for the School to store/hold my personal data including sensitive and personal information as detailed above.	

<b>Use of photos and videos</b>	<b>Tick</b> √
I am happy for the School to take, store or use photos and videos of me as detailed above.	

I understand that it is my responsibility to inform the School in writing if I decide to withdraw my consent.

Pupil's Name (Please print) .....

Sign..... Date .....



## Welcome to our Open Morning

Name of Parents:		
Child's Name:		
DOB:		
Email:		
Present School/Nursery		Current Year Group:
Any Extra Requirements/SEN		

I / We understand that the personal data provided above will be processed for the legitimate business of Kingswood House School whilst managing the admissions process. I / We understand that this information will be held until such time as the above-named child is no longer of an age to apply for a place at the School, or until I / we request that our personal data no longer be retained. ☐

I / We agree to you keeping in touch about admissions-related information (future deadlines and admissions events), news about and activities on offer at Kingswood House School. ☐

We will never sell your data and we promise to keep your details safe and secure.

You can change your mind at any time by emailing [admissions@kingswoodhouse.org](mailto:admissions@kingswoodhouse.org)

For further details on how your data is used and stored please visit Kingswood House School website.

Further Comments	
<b>FOR STAFF USE ONLY:</b>	
Tour Guides	