ORLEY FARM
SCHOOL

Data Protection Policy
for
Parents and pupils

First Issued:	September 2009	**Next Review:**	Autumn Term 2024
Last Reviewed:	Autumn Term 2023	**Version:**	5.0
Responsible:	Director of Operations		

1. INTRODUCTION

a. Data protection is an important legal compliance issue for Orley Farm School ("the 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. The School, as "data controller", is liable for the actions of its staff and Governors in how they handle data. It is therefore an area where all staff have a part to play in ensuring the School complies with and are mindful of its legal obligations, whether that personal data handling is sensitive or routine.

b. The school is fully committed to comply with the requirements of the Data Protection Act 2018 ("the Act") and General Data Protection Regulations (GDPR). The School will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants or members of the School who have access to any personal data held by or on behalf of the School, are fully aware of and abide by their duties and responsibilities under the Act.

c. This policy sets out the School's expectations and procedures with respect to processing any personal data it collects from data subjects (e.g. including parents, pupils, employees).

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

1. **Data controller** – an organisation that determines the purpose and means of the processing of personal data. For example, the School is the controller of pupils' personal information. As a data controller, the School is responsible for safeguarding the use of personal data.

2. **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll provider or other supplier of services.

3. **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. **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.

5. **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.

6. **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.

2. The Principles

a. 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.

b. 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:

1. Keeping records of our data processing activities, including by way of logs and policies;

2. Documenting significant decisions and assessments about how we use personal data; and

3. Generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notices were updated, how and when data protection consents were collected from individuals, how breaches were dealt with, etc.

3. Communications Manager

a. The School has appointed a person responsible for communications who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the GDPR. In the absence of such an appointed person, 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 Director of Operations via their PA.

4. Types of Personal Data Processed by the School

a. The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including by way of example, but not exclusively:

1. names, addresses, telephone numbers, e-mail addresses and other contact details;

2. bank details and other financial information;

3. past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;

4. where appropriate, information about individuals' health, and contact details for their next of kin;

5. references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and

6. images of pupils engaging in school activities, and images captured by the school's CCTV system;

b. Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources.

5. Sensitive Personal Data

a. The School may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sex life, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the school with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

6. Use of Personal Data by the School

a. The School will use personal data about individuals for a number of purposes as part of its operations, including as follows:

1. For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;

2. To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community;

3. For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the school's performance;

4. To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;

5. To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;

6. To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

7. To monitor (as appropriate) use of the school's IT and communications systems in accordance with the School's Acceptable use of Telephones, Cameras, E-Mail Systems and Internet policies;

8. To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's taking, storing and using images of children parental consent form;

9. For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and

10. Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

7. Data Accuracy and Security

a. 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 must notify the School's Communications Manager of any changes to information held about them.

b. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the Communications Manager in writing.

c. The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, ensuring that it is held in accordance with the Principles of the Act. All staff will be made aware of this policy and their duties under the Act.

8. Safeguarding Practice and Information Sharing

a. Whilst the Act places duties on organisations and individuals to process personal information fairly and lawfully, it is not a barrier to sharing information where the failure to do so would result in a child or vulnerable adult being placed at risk of harm. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

b. For further information, see HM Government's "Information sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers" (March 2015). The Local Safeguarding Children Board (LSCB) can require an individual or body to comply with a request for information, as outlined in section 14B of the Children Act 2004. This can only take place when the information requested is for the purpose of enabling or assisting the LSCB to perform its functions.

c. Any request for information about individuals should be necessary and proportionate to the reason for the request and should be made to Designated Safeguarding Lead.

9. Rights of Access to Personal Data ("Subject Access Request")

a. Individuals have the right under the Act to access personal data about them held by the School, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the Communications Manager, or in their absence, to the Director of Operations via their PA.

b. The School will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within statutory time-limits. As per the Information Commissioner's Office guidelines, a fee will be charged for this.

c. If an individual believes that any information held on him or her is incorrect or incomplete, then they should write to the Communications Manager as soon as possible, or in their absence, to the Director of Operations via their PA. The School will promptly correct any information found to be incorrect.

d. Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making. Pupils aged 13 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis.

e. A person with parental responsibility will generally be expected to make a subject access request on behalf of pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

f. **Exemptions.** All members of the school community should be aware that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may, in certain circumstances, be disclosed), nor any reference given by the School for the purposes of the education, training or employment of any individual.

10. Keeping in Touch and Supporting the School

a. With permission of parents, alumni, and other members of the school community, the School will use their contact details to keep them updated about the activities of the School.

b. Should you wish to cease to receive aforesaid updates, or would like further information about them, please contact the Communications Manager in writing, or in their absence, to the Director of Operations via their PA.

11. Pupils' Rights

a. The rights under the Act belong to the individual to whom the data relates. However, the School will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted.

b. In general, the School will assume that pupils' consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

c. However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School will maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example, where the school believes disclosure will be in the best interests of the pupil or other pupils.

d. Pupils are required to respect the personal data and privacy of others, and to comply with the school's E-Safety policy.

12. Queries and Complaints

a. Any comments or queries on this policy should be directed to the Communications Manager using the following contact details:
Communications Manager, Orley Farm School, South Hill Avenue, Harrow on the Hill, HA1 3NU

b. If the school does not have an appointed Communications Manager at the time of making a query or complaint, the matter will be dealt with by the Director of Operations.

c. If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the School complaints/grievance procedure and should also notify the Director of Operations.