ORLEY FARM
SCHOOL

Data Protection Policy
for
Parents and Pupils

First Issued:	September 2009	**Next Review:**	Spring Term 2027
Last Reviewed:	Spring Term 2026	**Version:**	6.0
Responsible:	Communications Manager & 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 the UK version of the General Data Protection Regulations (UK 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).

2. Definitions

Key data protection terms used in this policy are:

a. **(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 (including by its governors) is the controller of pupils' personal information. As a data controller, the School is responsible for safeguarding the use of personal data. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.

b. **(Data) Processor** – an organisation that processes personal data on behalf of a controller, for example a payroll provider or IT 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.

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

d. **Personal information (or personal data):** any information relating to a living individual (a data subject), by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

e. **Processing** – virtually anything done with personal data, 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.

f. **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.

3. Policy Application

a. 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).

b. 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.

c. 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 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

d. Where the School shares personal data with third party controllers – which may range from other schools, to parents, and appropriate authorities – 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.

4. Communications Manager

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 applicable data protection legislation. 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 Communications Manager at communication@orleyfarm.harrow.sch.uk.

5. The Principles

a. The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and 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 UK GDPR's broader '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, when staff training was undertaken,

how and when data protection consents were collected from individuals, how personal data breaches were dealt with, whether or not reported (and to whom), etc.

6. Lawful Grounds for Data Processing

a. Under the UK 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 the UK 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.
b. 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 the UK GDPR requires.
c. Other lawful grounds include:

    i. compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
    ii. contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
    iii. 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.

7. Responsibilities of all Staff

a. <u>Record-Keeping</u>

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff 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.

b. <u>Data Handling</u>

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

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.

c. Avoiding, Mitigating and Reporting Data Breaches

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

In addition, 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 the Communications Manager. 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.

d. Care and Data Security

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles, 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 they 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 the Communications Manager, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

e. Use of Third Party Platforms / Suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). Any request to engage a third party supplier should be referred to the Head of Communications Manager in the first instance, and at as early a stage as possible.

8. 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 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 the Communications Manager 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 the Communications Manager as soon as possible.

9. 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.

- Access to the School's Management Information System (MIS) requires two-factor authentication.
- Any information accessed or downloaded from the MIS is date-stamped with the user's name.
- Staff have restricted access to the MIS dependent on their role.
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- No third parties are permitted to take data offsite on personal devices.
- The School has anti-virus software and ransomeware protection through Sophos to prevent loss or damage to personal data, in addition to multiple back-up systems, one being off-site.
- Use of personal email accounts by staff for official School business is not permitted.

Digital/video images play an important part in learning activities. Pupils and staff members may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only the child's first name/initials will be used.

The school will comply with the Act and request parents'/carers' permission before taking images of pupils. We will also ensure that when images are published that the use of their names cannot identify the young people.

Parents/carers are requested to sign a Parental Consent Form to allow the school to take and use images of their children upon joining the school and also when their child transitions to Middle School and Upper School.

Recording and Photographing Children at School Events

i. EYFS (Reception):
No mobile phones or personal recording devices are to be used at EYFS events. This aligns with best practice guidance for settings caring for under 5s. The school will use registered devices to capture images for parents where appropriate.

ii. KS1 and above:
We will ensure one of the following happens at school-based events:
   a. Any paperwork sent out by the School will state clearly that images captured by parents are for household use only (e.g., family albums or private social media accounts with appropriate privacy settings), or
   b. Staff will read a short, prepared statement at the start of events so that the message to parents is consistent.

9. Types of Pupil and Parent 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.