

Privacy Notice for Staff



Reviewed by: Bursar, July 2026

Next review by: July 2027

1 Introduction

- 1.1 The Godolphin and Latymer School Foundation, in its capacity as trustee of the Godolphin and Latymer School (together the “School”), is a Data Controller for the purposes of Data Protection Law¹, which means it determines how an individual’s personal data is processed and for what purposes.
- 1.2 This Notice applies to current, former and prospective employees and, where applicable, governors, volunteers, contractors, casual workers, visiting teachers and agency staff engaged by the School.
- 1.3 During the course of the School’s activities, the School will process Personal Data about you. This Notice explains how and why the School collects and processes Personal Data about you, including how it is collected, used, shared and retained. It applies alongside any other privacy information the School may provide about a particular use of Personal Data, for example when collecting information via an online or paper form.
- 1.4 The Bursar, supported by the Head of Legal and Compliance, is responsible for overseeing data protection within the School. They will deal with any requests or enquiries about how the School processes your Personal Data and endeavour to ensure that your Personal Data is processed in compliance with this Notice and Data Protection Law. The Bursar and Head of Legal and Compliance can both be contacted via email at DPOfficer@godolphinandlatymer.com.
- 1.5 This Notice does not form part of any contract of employment or other agreement with the School.

2 Types of Personal Data processed by the School

- 2.1 **Personal Data** means any information relating to a living individual who can be identified, either directly or indirectly. Examples of the personal data which the School may process about you include:
 - name, addresses, date of birth, telephone numbers, e-mail addresses and other contact details;
 - identity and right-to-work information, including copies of passports, visas and other identification documents;
 - bank details and other financial information regarding payment of your salary, expenses and benefits, and the administration of your pension;
 - National Insurance, tax and payroll information;
 - information about your health, wellbeing, sickness absence, fitness for work and any reasonable adjustments, together with emergency contact details for your next of kin;
 - equality and diversity information, including information about your racial or ethnic origin, religious or philosophical beliefs, disability and sexual orientation, where collected;
 - biometric information (see more on this below);

¹ This includes the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and the Data (Use and Access) Act 2025, together with any legislation that amends or replaces them.

- references given or received by the School about you;
- correspondence and other communications with or about you;
- information collected during the recruitment process, including your application, employment history, education, qualifications, professional achievements, interview records and information about your suitability for the position applied for;
- information relating to professional memberships, registrations and training;
- information relating to criminal convictions, offences or allegations, including information obtained through Disclosure and Barring Service (DBS), Barred List and other safer recruitment checks;
- information about your employment, job performance, contract, salary, working hours, attendance, training, skills, achievements, appraisal, career progression and disciplinary or capability matters;
- other employment related information, including flexible working requests, maternity, paternity, adoption or parental leave requests, or requests for compassionate leave;
- information relating to grievances, complaints, investigations, safeguarding concerns or allegations involving you;
- vehicle details if you are using the School's parking facilities;
- photographs, audio and video recordings and images captured by the School's CCTV system;
- information about your use of the School's IT and communications systems, including account, access, filtering and monitoring information; and
- opinions or other information recorded about you.

Some of the information listed above is Special Category Personal Data or criminal offence data and is subject to additional requirements under Data Protection Law.

2.2 The School may collect your Personal Data in a number of ways. For example:

- you may provide the School with Personal Data about yourself, including during the recruitment, appointment and induction processes and throughout your employment;
- Personal Data may be created internally by the School during the course of employment. This includes employment records, correspondence and information generated through the use of the School's systems, access controls and CCTV; and
- Personal Data may be obtained from third parties or publicly available sources, including referees, previous employers, recruitment agencies, the DBS, professional bodies, public authorities, pension and benefits providers, occupational health providers and online searches undertaken as part of the recruitment process where applicable.

2.3 Some Personal Data requested by the School is required to enable the School to enter into or perform a contract with you or to comply with its legal obligations. This includes, where applicable, information required to confirm your identity and right to work, administer payroll and tax, and complete safeguarding and safer recruitment checks. If you do not provide information that is required, the School may be unable to consider your application, employ or engage you, provide certain employment benefits or comply with its legal obligations.

3 Why the School needs to process your Personal Data

3.1 The School will process a wide range of Personal Data about current, former and prospective staff in order to operate the School and manage its relationship with you.

3.2 Depending on the purpose and circumstances, the School will rely on one or more of the following lawful bases when processing your Personal Data:

- the processing is necessary to take steps at your request before entering into a contract or to perform a contract with you;
- the processing is necessary to comply with a legal obligation;
- the processing is necessary for the School's legitimate interests or those of another person, except where those interests are overridden by your interests, rights or freedoms;
- the processing is necessary for a recognised legitimate interest under Data Protection Law, for example in certain circumstances involving safeguarding, crime prevention or emergencies;
- the processing is necessary to protect your vital interests or those of another person; or
- you have given your consent, where consent is appropriate.

3.3 Where the School relies on legitimate interests, it will consider whether the processing is necessary and balance those interests against the potential impact on you. The School's legitimate interests include managing and operating the School effectively, supporting staff, protecting the School community and its property, maintaining the security of its systems, establishing and defending legal rights, and promoting the School's interests and objectives.

3.4 The School processes Personal Data for purposes including:

- carrying out HR, administrative and management functions and managing your recruitment and employment, administering payroll, tax, National Insurance, benefits and pensions, managing attendance and leave, monitoring performance and providing references;
- complying with immigration and right-to-work requirements, including any applicable sponsorship obligations;
- enabling relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- safeguarding and promoting the welfare of staff and pupils, including recording concerns that may not meet a statutory threshold but are reported to the School's Designated Safeguarding Lead in accordance with the School's safeguarding procedures;
- providing training and support to staff and arranging work-related travel and School visits;
- filtering and monitoring, where appropriate, your use of the School's IT and communications systems in accordance with the School's Acceptable Use of ICT for Staff Policy;

- using photographs, video or audio recordings of staff for teaching, communication, marketing and promotion purposes, including in School publications, on social media and on the School website;
- providing a safe and secure environment, including the use of CCTV in accordance with the School's CCTV Policy, using biometric information for attendance, fire safety and cashless catering purposes, where applicable;
- contacting your next of kin or emergency contact where necessary, including in an emergency;
- carrying out or cooperating with any internal or external complaints, disciplinary, grievance, capability or investigation process;
- protecting and promoting the School's interests and objectives;
- maintaining relationships with staff alumni and the School community, including direct marketing or fundraising activity; and
- obtaining appropriate professional advice and insurance for the School and establishing, exercising or defending legal claims.

3.5 The School also processes Special Category Personal Data, including information about health, disability and biometric information used for identification purposes, and criminal offence data, including information obtained through DBS and other safer recruitment checks. Where the School processes Special Category Personal Data, it will only do so where it has an Article 6 lawful basis and an additional condition under Article 9 UK GDPR and, where required, Schedule 1 of the Data Protection Act 2018. Criminal offence data will only be processed where permitted by Data Protection Law and appropriate safeguards are in place. The reasons for processing this data include:

- carrying out DBS, Barred List and other safer recruitment checks;
- meeting the School's obligations and exercising rights in connection with employment, including managing sickness absence, assessing fitness for work and providing reasonable adjustments;
- registering you on site for attendance and fire safety purposes and enabling cashless purchases from the dining room, where applicable;
- monitoring equality of opportunity or treatment, where applicable;
- protecting your vital interests or those of another person where you are physically or legally incapable of giving consent; and
- meeting legal and regulatory requirements relating to safeguarding, public health and health and safety and the School's duties of care.

3.6 Examples of when the School might seek your specific consent, or where required, explicit consent to use your Personal Data include:

- ***Photographs and video recordings:*** Most uses of photographs, audio or video recordings as described above will not require your consent. However, if the School considers that a proposed use is more privacy intrusive, we may ask for your consent before using a specific image or recording.
- ***Medical information:*** The School operates an entirely voluntary scheme under which information about a member of staff's medical conditions, allergies and medication can be held securely and confidentially in the Medical Centre in the event that they are unable to give this to the emergency services during a medical

emergency. As this is voluntary, your explicit consent will be requested when you provide the data.

- **Biometric Data:** The School will seek your explicit consent before using your biometric information for identification purposes. If you do not give consent, or later withdraw it, you will be provided with a PIN or card as an alternative. Further information is set out in the School's Biometric Information Notice.

3.7 Further information about the School's lawful bases for processing Personal Data, Special Category Personal Data and criminal offence data is set out in the Data Protection Policy.

4 Security of personal data and sharing with third parties

4.1 Personal Data will only be accessed within the School by individuals who need it for their role and in accordance with the School's access controls. Particularly strict access controls apply to medical information. Detailed medical information held by the Medical Centre will normally only be accessed by the School Medical Team. Health information held for employment purposes, including sickness absence records and occupational health information, may be accessed by the HR Office and relevant managers, but only where necessary and limited to the information they need for their responsibilities.

4.2 The School will take reasonable steps to ensure that your Personal Data is accurate and, where necessary, kept up to date. You must notify the School of any relevant changes to your Personal Data and you may also be asked to review and update your records.

4.3 The School will take appropriate technical and organisational measures to ensure the security of Personal Data, including policies around use of technology and devices and access to School systems. In particular, all staff must be familiar with the School's Information Security Policy, available in the 'Policies' folder via a link from the Staff Handbook.

4.4 The School may share your Personal Data with third parties where there is a lawful basis for doing so. Only the Personal Data necessary for the relevant purpose will be shared. Recipients may include:

- banks, BACS and payment providers in order to pay salaries and expenses;
- HM Revenue and Customs and other tax authorities in connection with payroll, tax and National Insurance requirements;
- pension, benefits and payroll providers;
- occupational health providers and other medical professionals where a referral, assessment or medical advice is required;
- auditors and accountants;
- the School's legal advisers, insurers, insurance brokers and other professional advisers;
- organisations providing training or involved in School visits and other School activities in which you participate; consultants and experts engaged to support the School where the Personal Data is relevant to their work;
- providers of IT, communications, cloud storage and other services used by the School;
- referees, prospective employers and other organisations requesting or providing employment references;

- the Disclosure and Barring Service, and other organisations involved in safer recruitment or employment checks; and government departments, public authorities, local authorities, law enforcement bodies and regulators, including the LADO, the police and the Independent Schools Inspectorate, where applicable.
- 4.5 The School is required or permitted under Data Protection Law, other legislation and statutory guidance to record or report certain incidents, concerns or allegations that arise or are reported. Records may be kept whether or not a concern or allegation is substantiated or meets the threshold for referral to an external authority. This may include notes on HR or safeguarding files, and, where the relevant threshold is met or disclosure is otherwise required or appropriate, referrals to external bodies such as the LADO, the Disclosure and Barring Service, the Teaching Regulation Agency or the police. For further information about this, please see the School's Safeguarding (Child Protection) Policy.
- 4.6 The School may transfer your Personal Data outside the UK in connection with obtaining or providing references or other pre-employment information, organising overseas School visits or communicating with you when you are overseas. Your Personal Data may also be accessed or stored outside the UK by providers of cloud services, such as Google or Microsoft 365. Where Personal Data is transferred outside the UK, the School will ensure that the transfer is permitted under Data Protection Law and that appropriate safeguards are in place, such as UK adequacy regulations or an approved international transfer mechanism. Further information about the safeguards used by the School may be obtained from the Bursar or Head of Legal and Compliance.
- 4.7 Some processing of Personal Data is carried out on the School's behalf by service providers, including providers of IT systems, communications, website and cloud-storage services. Where a service provider processes Personal Data on the School's behalf, the School will put appropriate contractual arrangements in place requiring the provider to process Personal Data only in accordance with the School's instructions and to keep it secure.

5 How long we will keep your personal data

- 5.1 The School will retain Personal Data securely and only for as long as necessary for the purposes for which it was collected, including to meet the School's legal, regulatory, safeguarding, employment and contractual obligations. Different retention periods apply to different categories of Personal Data. Personal Data will be securely deleted or destroyed when it is no longer required, in accordance with the School's Record Keeping and Retention Policy and Retention Schedule.
- 5.2 If you have any specific queries about how the School's retention requirements are applied or wish to request that Personal Data that you no longer believe to be relevant is considered for erasure, please contact the Bursar or Head of Legal and Compliance at DPOfficer@godolphinandlatymer.com. However, please bear in mind that the School may have lawful and necessary reasons to retain some Personal Data even following such a request.
- 5.3 Please refer to the School's Record Keeping and Retention Policy for more information.

6 Your rights regarding your Personal Data

- 6.1 Under Data Protection Law, you have the right to request access to the Personal Data the School holds about you. Please contact the Bursar or Head of Legal and Compliance at

DPOfficer@godolphinandlatymer.com. Further information is available in the School's Subject Access Request Procedure.

6.2 Subject to the conditions and exemptions under Data Protection Law, you may also have the right to:

- ask the School to correct inaccurate or incomplete Personal Data;
- ask the School to erase your Personal Data in certain circumstances;
- ask the School to restrict the processing of your Personal Data in certain circumstances; and
- receive certain Personal Data in a portable format or ask for it to be transferred to another organisation in certain circumstances.

These rights are not absolute, and the School may lawfully continue to process or retain Personal Data in some circumstances.

6.3 Where the School relies on your consent to process your Personal Data, you have the right to withdraw your consent at any time by contacting the Bursar or Head of Legal and Compliance. Withdrawal will not affect the lawfulness of processing carried out before consent was withdrawn. Please be aware, however, that the School may have another lawful basis to process the Personal Data in question without relying on your consent.

6.4 **Right to object:** You have the right to object to the processing of your Personal Data in certain circumstances, including where the School relies on legitimate interests. You have an absolute right to object to the use of your Personal Data for direct marketing.

7 Further information and guidance

7.1 The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights or how the School processes your Personal Data will be brought to your attention in an appropriate manner.

7.2 If you believe that the School has not complied with this Privacy Notice or has otherwise failed to comply with Data Protection Law, you should raise your concerns with the Bursar at DPOfficer@godolphinandlatymer.com. A complaint may be made orally or in writing. The School will acknowledge the complaint within 30 days, take appropriate steps to investigate it and respond without undue delay. Where appropriate, the School will keep you informed of the progress of its investigation and will notify you of the outcome. If you remain dissatisfied, you have the right to lodge a complaint with the Information Commissioner's Office (ICO). The ICO recommends that you give the School an opportunity to resolve the matter before involving the regulator.