

PLYMOUTH COLLEGE
PRIVACY NOTICE
Including Early Years Foundation Stage



Last reviewed:	August 2026
Next review date:	August 2027
Responsibility:	Head of Systems & IT - DPO

WHO WE ARE

- Plymouth Education Limited, a company, limited by shares registered in England and Wales (company number 16067801), whose registered office is Ford Park, Plymouth, Devon, PL4 6RN.*

We educate children from the ages of 3–18, and this Privacy Notice applies to the entirety of Plymouth College (the “School”), comprising Senior, Prep, and Early Years Foundation Stage (EYFS).

The School processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), and, where applicable, the Data (Use and Access) Act 2025 (DUAA 2025), which introduced targeted reforms to the UK data protection landscape.

WHAT THIS PRIVACY NOTICE IS FOR

This Privacy Notice explains how the School collects, uses, stores, and shares personal data about individuals, including its staff; current, past and prospective pupils; and their parents, carers or guardians (collectively referred to as “parents”).

It is issued in compliance with UK data protection law, comprising primarily the UK GDPR and the Data Protection Act 2018, with reference to reforms introduced by the Data (Use and Access) Act 2025 where relevant.

This Privacy Notice should be read alongside any other privacy information provided by the School, for example when collecting personal data via an online or paper form.

It also applies in addition to the School’s other relevant policies and contractual documents, including:

- Any contract between the School and its staff, or between the School and parents of pupils;
- The School’s Taking, Storing and Using Images of Pupils Policy;
- The School’s CCTV Policy;
- The School’s Record Keeping Policy;
- The School’s safeguarding, pastoral, and health and safety policies, including how concerns or incidents are recorded; and
- The School’s IT policies, including the Acceptable Use Policy, Data Protection Policy, and E-Safety Policy.

All individuals working for, or acting on behalf of, the School (including staff, volunteers,

members of the Local Advisory Board (LAB), and service providers) are required to comply with this Privacy Notice and the School's Staff Data Protection Policy, which provides additional detail on how personal data about those individuals is used.

RESPONSIBILITY FOR DATA PROTECTION

The School has appointed **Mr James Moate** as its **Data Protection Officer (DPO)**. The DPO is responsible for overseeing compliance with this Privacy Notice and Data Protection Law, including the **UK GDPR, Data Protection Act 2018**, and the **Data (Use and Access) Act 2025 (DUAA 2025)**.

The DPO ensures the School maintains appropriate Data Protection Impact Assessments (DPIAs) for new or high-risk processing activities, as required by Article 35 of the UK GDPR, and upholds its duty of accountability through documented records of processing activities (ROPAs) under Article 30.

All requests or enquiries regarding the School's use of personal data, including data rights requests (see section "Your Rights" below), should be directed to:

Mr James Moate, Data Protection Officer

Email: privacy@plymouthcollege.com

Address: Plymouth College, Ford Park, Plymouth, Devon, PL4 6RN.

WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

In order to carry out its ordinary duties to staff, pupils, parents, and the wider School community, the School needs to collect, store, and process personal data about individuals as part of its daily operations. The School processes personal data in accordance with the UK GDPR and the Data Protection Act 2018, which together require that processing is lawful, fair, and transparent, and that individuals are clearly informed of the purposes for which their data is used.

Some processing is required for the School to meet its legal obligations or to perform contractual duties, for example, under an employment contract or a contract with parents for the education of their child.

Other processing may be based on the School's legitimate interests, or those of a third party, where these are not overridden by the rights and freedoms of the individual. Where processing involves special category personal data, the School will also identify an appropriate condition under Article 9 of the UK GDPR in addition to the Article 6 lawful basis.

The School's legitimate interests include:

- Pupil selection, admissions, and confirmation of identity;
- Delivery of education and co-curricular provision;
- Pastoral, safeguarding, and welfare support;
- Management planning, research, and statistical analysis (including gender pay, diversity, and equality monitoring);
- Communication with alumni, donors, and the School community;
- Security and site management, including CCTV monitoring; and

- Ensuring effective governance, audit, and risk management.

The School may also process special category personal data and criminal records data (under Articles 9 and 10 of the UK GDPR respectively) where necessary to meet its statutory duties or to safeguard pupils' welfare, for example, for safeguarding, employment checks (including DBS checks), and provision of health or special educational needs (SEN) support.

The School maintains records of processing activities (ROPAs) and undertakes Data Protection Impact Assessments (DPIAs) when introducing new systems or activities that may pose a high risk to individual privacy, as required by Articles 30 and 35 of the UK GDPR.

TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

The School processes a range of personal data, which may include (as appropriate):

- Names, addresses, telephone numbers, email addresses, and other contact details;
- Car registration and parking information;
- Bank details and other financial data (e.g. for fee payments, payroll, or expenses);
- Academic, disciplinary, and attendance records (including information about special educational needs or learning support requirements);
- Employment and personnel records, including training, appraisals, and safeguarding checks;
- Health and welfare data, including relevant medical or dietary information and next of kin details;
- Correspondence and records of communications with or about pupils, parents, and staff;
- References, reports, and professional assessments;
- Photographic and video images, including CCTV footage, in accordance with the School's Taking, Storing and Using Images of Pupils Policy; and
- Digital activity records generated by use of School systems (such as login data, email usage, or device access logs) where monitored in accordance with the School's IT Acceptable Use Policy.

The School collects only personal data that is adequate, relevant, and limited to what is necessary for the purpose for which it is processed, in accordance with the data minimisation principle under Article 5(1)(c) of the UK GDPR. The accuracy and retention of data are reviewed periodically as part of the School's accountability obligations.

HOW THE SCHOOL COLLECTS DATA

The School collects personal data in several ways, most commonly:

- Directly from the individual (or, in the case of pupils, from parents or carers) through forms, applications, assessments, or day-to-day correspondence;
- From third parties such as previous schools, local authorities, health professionals, or safeguarding partners who lawfully share information; and
- From publicly available sources, where appropriate for due diligence or regulatory purposes.

Where personal data is obtained from a source other than the individual themselves, the School will inform the individual of the source and purpose of the data as required by Article 14 of the UK GDPR, unless an exemption applies.

The School does not use automated decision-making or profiling in a way that produces legal or similarly significant effects on individuals without human involvement, as required by Article 22 of the UK GDPR. Should any such tools be introduced in future, for example, for admissions analysis or safeguarding risk assessment, the School will conduct a DPIA and inform affected individuals in advance.

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

The School limits access to personal data strictly on a need-to-know basis, ensuring that only authorised individuals or organisations may process it for legitimate and defined purposes.

Personal information may be shared, where necessary, with:

- Professional advisers (e.g. legal, insurance, communications, or financial consultants);
- Government and statutory authorities (e.g. HMRC, DfE, police, and local authorities);
- Regulatory and inspection bodies (e.g. Independent Schools Inspectorate, the Charity Commission, or the Information Commissioner's Office); and
- Approved service providers and data processors (e.g. IT system suppliers, cloud hosting services, or payment processors).

All third-party processors operate under a formal data processing agreement in compliance with Article 28 of the UK GDPR, which requires clear definition of processing purposes and duration, security and confidentiality guarantees, and the processor to act only on the School's documented instructions.

In specific cases, such as safeguarding or SEN support, information may be shared more widely with authorised staff or contractors to ensure pupil welfare.

The School does not transfer personal data outside the UK unless adequate protection measures are in place. Where international transfer is necessary (for example, through an overseas cloud storage provider), it will only occur under a valid transfer mechanism, such as the UK International Data Transfer Agreement (IDTA) or recognised adequacy decision.

All access to sensitive categories of information, including medical, financial, and safeguarding records, remains strictly controlled and logged in accordance with the School's Information Security Policy.

Debt Management and Credit Control - To ensure the financial sustainability of the school and the wider Galaxy Global Education group, we may share information regarding outstanding fees and debtor balances with Galaxy Global Education Ltd.

This information includes parent/guardian contact details, student names (for account identification), and the total outstanding balance. We do this under our **Legitimate Interests (UK GDPR Article 6(1)(f))** for the purposes of group-level credit control and debt recovery.

The School operates a strict information barrier to ensure that financial data is accessible only to authorised group finance personnel and is not shared with teaching or academic staff, so that a family's financial circumstances have no bearing on a student's educational experience or treatment within the School.

HOW LONG WE KEEP PERSONAL DATA

The School retains personal data only for as long as necessary to fulfil the purpose for which it was collected, to meet legal or contractual obligations, or to support legitimate operational or historical interests. Retention periods are defined in the School's Records Retention Schedule, which is reviewed annually.

Typical retention periods include:

- Staff and pupil personnel files — up to 7 years following departure;
- Financial and payroll records — up to 7 years for audit and tax compliance;
- Safeguarding and child protection records — retained in accordance with statutory requirements (currently until the individual reaches the age of 25, or longer if directed by legislation); and
- Governance and policy documentation — retained in line with the School's compliance and historical archiving obligations.

The School conducts periodic retention reviews to identify data that is no longer required, and applies secure disposal methods for all formats (digital, paper, and backup). Where the School continues to hold personal data beyond its normal retention period, for example, for safeguarding, legal claims, or archiving in the public interest, such data is kept under restricted access with a documented justification recorded by the Data Protection Officer.

Individuals retain the right to request erasure of their data under Article 17 of the UK GDPR; however, the School may retain data where a lawful reason applies (e.g. safeguarding, employment law, or contractual necessity). For queries about data retention or erasure, please contact the Data Protection Officer at privacy@plymouthcollege.com.

KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The School and its associated community networks (such as alumni and parent associations) may contact parents, carers, alumni, and supporters about relevant School activities — including events, fundraising, and community updates — where there is a lawful basis to do so under the UK GDPR.

The lawful basis for such communications will typically be consent (under Article 6(1)(a) of the UK GDPR) or, where appropriate, legitimate interests. The School maintains clear records of when and how consent for communications was obtained or withdrawn.

Individuals may withdraw their consent or object to communications at any time by contacting the School at privacy@plymouthcollege.com. Upon withdrawal, the School will cease sending non-essential communications and will retain only a minimal suppression record to ensure compliance with the individual's preference.

The School does not sell or share personal contact information for marketing purposes. All communications will clearly identify the School as the sender and include an easy mechanism to opt out.

YOUR RIGHTS

Individuals have the following rights under the UK GDPR and the Data Protection Act 2018 in relation to their personal data. All requests should be made in writing to the Data Protection Officer at privacy@plymouthcollege.com. The School will respond within one calendar month of receipt. For complex or multiple requests, this period may be extended by a further two months; where an extension is necessary, the School will notify the individual within the first month and explain the reason for the delay.

Right of access

(Article 15): Individuals may request a copy of the personal data the School holds about them and information about how it is processed.

Right to rectification

(Article 16): Individuals may request correction of personal data that is inaccurate, out of date, or incomplete.

Right to erasure

(Article 17): Individuals may request deletion of their personal data in certain circumstances, for example, where the data is no longer necessary for the purpose for which it was collected.

Right to restriction of processing

(Article 18): Individuals may request that the School restricts processing of their data in certain circumstances, for example, while the accuracy of the data is contested.

Right to data portability

(Article 20): Where processing is based on consent or a contract and is carried out by automated means, individuals may request their data in a structured, machine-readable format.

Right to object

(Article 21): Where the School relies on legitimate interests as the lawful basis, individuals may object to processing for reasons connected to their particular situation. The School must stop processing unless it can demonstrate compelling legitimate grounds that override the individual's interests, rights and freedoms, or the processing is necessary for legal claims. Individuals have an unconditional right to object to processing for direct marketing at any time.

Rights related to automated decision-making

(Article 22): Individuals have the right not to be subject to decisions made solely by automated processing that produce legal or similarly significant effects.

Right to withdraw consent

Where the School relies on consent to process personal data, individuals may withdraw that consent at any time. Withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

Right to lodge a complaint

(Article 77): Individuals have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk if they consider that the School's processing of their personal data infringes UK data protection law.

Certain exemptions apply, for example, where disclosure would reveal another individual's personal data, breach legal privilege, or contravene safeguarding or examination regulations. The School will record and explain any reliance on such exemptions.

Pupils may exercise their rights where, in the School's opinion, they have sufficient maturity to understand their request. Requests from parents or guardians on behalf of pupils will be assessed in light of the child's best interests and applicable data protection rights.

While parents may not have an automatic statutory right to all information about a child, the School will continue to share appropriate educational and pastoral information under the Parent Contract or where it is in the child's legitimate interests to do so.

Where the School relies on consent to process personal data, for example, for certain images or fundraising, individuals may withdraw that consent at any time. Withdrawal will be recorded and acted upon promptly.

DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held about an individual is as accurate, relevant, and up to date as possible. Individuals should promptly notify the School Office in writing of any changes to personal details, such as contact information, health details, or authorised emergency contacts, so that records remain current.

Under the UK GDPR and the Data Protection Act 2018, individuals have the right to request that any personal data which is inaccurate, outdated, or incomplete be corrected or securely erased. Such requests should be directed to the Data Protection Officer at privacy@plymouthcollege.com and will be actioned within one calendar month, unless a lawful exemption applies.

The School takes robust technical and organisational measures to safeguard all personal information, including encryption, secure storage, access controls, and regular review of data systems. All staff, contractors, and members of the Local Advisory Board (LAB) receive mandatory data protection and cyber-awareness training annually and must confirm understanding of their obligations under the School's Data Protection Policy.

In the event of a suspected or confirmed personal data breach, the School will follow its Data Breach Management Procedure, including mandatory internal reporting, root cause analysis, and, where required, notification to the Information Commissioner's Office (ICO) within 72 hours of discovery and, where there is a high risk to individuals, notification to those affected, as required by Articles 33 and 34 of the UK GDPR.

The School conducts regular data security audits and risk assessments, reporting outcomes to the Local Advisory Board for oversight and assurance of compliance with statutory data protection duties.

THIS POLICY

The School reviews and updates this Privacy Notice and its underlying Data Protection Policy at least annually, or sooner if required by law, regulatory guidance, or changes in practice. The most recent version will be made available on the School's website and in the staff policy repository.

Any substantial changes affecting how personal data is collected, used, stored, or shared will be communicated promptly to affected individuals, together with an explanation of their rights under the UK GDPR and the Data Protection Act 2018.

The Local Advisory Board (LAB) has oversight of data protection compliance and receives annual assurance reports on data governance.

QUERIES AND COMPLAINTS

Any questions, concerns, or requests regarding this Privacy Notice or the School's handling of personal data should be directed to the Data Protection Officer:

Data Protection Officer:	Mr James Moate
Email:	privacy@plymouthcollege.com
Address:	Plymouth College, Ford Park, Plymouth, Devon, PL4 6RN

Complaints relating to data protection will be handled in accordance with the School's Data Protection Complaints Procedure. The School will acknowledge any complaint promptly and provide a full written response within one calendar month.

Individuals who believe the School has not acted in accordance with the UK GDPR or the Data Protection Act 2018 may escalate their concern to the Information Commissioner's Office (ICO):

ICO Helpline:	0303 123 1113
Website:	www.ico.org.uk
Address:	Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Oversight of the School's data protection compliance and complaints handling rests with the Local Advisory Board (LAB), which receives a summary of complaints and resolution outcomes annually to ensure transparency and continuous improvement.