PLYMOUTH COLLEGE

# DATA PROTECTION POLICY

Including Early Years Foundation Stage

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

## 1. Background

Data protection is an essential legal and regulatory requirement for Plymouth College ("the School"). During the course of the School's activities, it collects, stores, and processes personal data about staff, pupils, parents, suppliers, and other third parties (as detailed in the School's Privacy Notice). All staff share responsibility for ensuring compliance with relevant legal obligations and for handling personal data responsibly and securely.

This policy applies to all categories of data subjects, including current and former staff (employees, agency staff, contractors, and volunteers), pupils, parents, guardians, suppliers, and any other individuals whose personal data is processed by the School.

The law governing data protection has evolved, initially under the Data Protection Act 1998, then the EU General Data Protection Regulation (GDPR) implemented on 25 May 2018, and the UK Data Protection Act 2018 (DPA 2018). The Data Use and Access Act 2025 (DUAA 2025) introduces reforms to the UK data protection landscape, including changes to how organisations record processing activities, assess legitimate interests, and conduct Data Protection Impact Assessments. Some of these reforms are relevant to independent schools and the School will implement them as they come into effect. In the context of safeguarding, the School has an ongoing duty to ensure all personal data, including pupil data, is processed in a lawful, secure, and accountable manner.

The Information Commissioner's Office (ICO) remains the regulator responsible for enforcement. The School also complies with the UK's international data transfer requirements under the International Data Transfer Agreement (IDTA) and Addendum to the EU Standard Contractual Clauses, ensuring that any personal data transferred outside the UK receives equivalent protection.

All staff must comply with this policy. Accidental breaches may occur, but any breach must be reported promptly and could result in disciplinary action. This policy will be updated as necessary to reflect legislative changes.

This policy outlines the School's expectations and procedures for processing all personal data collected from data subjects (e.g., pupils, parents, guardians, and staff) in compliance with UK GDPR and the Data Protection Act 2018.

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

- **Data Controller** – an organisation that determines the purpose and means of processing personal data. For example, the School primarily acts as the Data Controller for personal

data relating to pupils, staff, parents, and other individuals connected with its operations. It is responsible for safeguarding the use of personal data.

- **Data Processor**—an organisation that processes personal data on behalf of a Data Controller, such as a payroll provider or other service supplier.
- **Personal data breach**—a security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- **Data Subject** – the person whose information is processed.
- **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, 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. This includes personal data contained in HR records, payroll information, performance documentation, and communications relating to staff employment.
- **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, and genetic or biometric data used to identify an individual. There are also separate rules for processing personal data relating to criminal convictions and offences (UK GDPR Article 10). All processing of special category data is documented under Schedule 1 of the Data Protection Act 2018, identifying the lawful condition relied upon (such as employment and social protection, safeguarding of children, or equality of opportunity). Access to special category data is restricted to authorised staff only, in accordance with the School's Access Control Policy
- **Ethical Firewall -** implemented through role-based access controls and restricted permissions within financial systems

## 2. Data Protection Officer

The School has appointed Mr James Moate as the Data Protection Officer (DPO), who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of UK GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred to the Data Protection Officer at privacy@plymouthcollege.com in the first instance.

## 3. The Principles

UK GDPR and the Data Protection Act 2018 set out six core principles for the lawful processing of personal data (Article 5, UK GDPR). All data controllers and processors must ensure that personal data is:

- Processed lawfully, fairly, and transparently;
- Collected for specified, explicit purposes and not used beyond those purposes;
- Adequate, relevant, and limited to what is necessary for the intended purpose;
- Accurate and kept up to date;
- Retained no longer than necessary for the purpose for which it was collected; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

The sixth principle, integrity and confidentiality, requires the School to implement both organisational and technical measures that ensure data remains protected against unauthorised or unlawful processing, accidental loss, destruction, or damage.

For details on retention periods and criteria, staff should consult the School's Data Retention Policy, available on the staff intranet or from the Data Protection Officer.

The accountability principle requires the School to demonstrate that all personal data processing is compliant. This includes, among other things:

- maintaining clear records of processing activities;
- maintaining staff HR files, recruitment records, payroll processing, and employment-related decision-making records;
- documenting assessments and decisions regarding personal data use; and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including, for example, when and how its Privacy Notice(s) were updated; data protection consents were collected from individuals; and any incidents or breaches, in line with UK GDPR and the Data Protection Act 2018.

## 4. Lawful grounds for data processing

Under UK GDPR and the Data Protection Act 2018, personal data may only be processed if there is a lawful basis. Where consent is relied upon as a lawful basis under Article 6(1)(a) UK GDPR, it must be freely given, specific, informed, and unambiguous — for example, a clear affirmative action such as ticking an opt-in box. Other grounds are often preferable where feasible.

Where the School processes special categories of personal data (UK GDPR Article 9), explicit consent is required unless another Schedule 1 condition of the Data Protection Act 2018 applies (such as employment, safeguarding, or public interest). Explicit consent involves a clear, affirmative, and specific statement of agreement.

A common lawful basis is 'legitimate interests' (Article 6(1)(f) UK GDPR), which requires careful balancing between the rights of the individual and the interests of the School. Data subjects have the right to object to such processing (see Rights of Individuals below), and the School must ensure transparency and proper assessment. The School's legitimate interests are described in its Privacy Notice, updated in line with current legislation.

Other lawful bases include:

- Compliance with a legal obligation, including employment, safeguarding, and diversity requirements;
- Performance of a contract — for example, with staff, parents, or suppliers. In the case of staff, this includes employment contracts, payroll administration, benefits provision, and HR management processes.
- Specific grounds for processing special categories of personal data (such as health information), including explicit consent, emergencies, and statutory public interest provisions, in accordance with UK GDPR and the Data Protection Act 2018.

## Use of Third-Party Data Processors

When the School engages third-party organisations to process personal data on its behalf, it ensures that these processors undergo rigorous due diligence and enter into legally binding Data Processing Agreements (DPAs) as required under Article 28 of UK GDPR. This includes processors handling staff-related data, such as payroll providers, pension administrators, recruitment platforms, and HR systems providers.

DPAs detail:

- The subject matter and duration of processing
- The nature and purpose of processing
- The types of personal data and categories of data subjects involved
- The rights and obligations of both the School and the processor

All processors must implement technical and organisational safeguards to protect personal data and are regularly monitored by the Data Protection Officer or Head of IT Systems.

Where high-risk processing occurs, including third-party involvement, the School performs Data Protection Impact Assessments (DPIAs) in line with Article 35 UK GDPR to identify and mitigate risks. The School maintains a standard DPIA template approved by the Data Protection Officer. A DPIA must be completed before any new high-risk system, vendor, or processing activity begins.

# Group Financial Governance - Non-staff

## Parent Financial Data

To ensure the financial sustainability of the School and the wider Galaxy Global Education group, we share information regarding outstanding fees and debtor balances with our parent company, 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.

This sharing is disclosed in the School's Privacy Notice for parents and guardians. Parents and guardians may object to this processing under Article 21 UK GDPR; the School will cease such processing unless it can demonstrate compelling legitimate grounds that override the individual's interests, rights, and freedoms.

We have implemented a strict "Ethical Firewall" to ensure that this financial information is only accessible to authorised group finance personnel and is never shared with teaching or academic staff. This ensures that a family's financial status has no impact on the student's educational experience or treatment within the classroom.

The Legitimate Interests Assessment is available on request or held by the Data Protection Officer.

# Group Financial Governance - Staff

## Staff Data

To ensure effective financial oversight, workforce planning, and budget reconciliation across the Galaxy Global Education Ltd group, we share limited professional information about our employees with our parent company, Galaxy Global Education Ltd.

**What data is shared:** We only share your full name, job title/role, and your salary or employment cost. We do not share sensitive personal information such as your home address, bank details, or any disciplinary or medical records for these purposes.

**Purpose of sharing:** This data is used strictly for group-level financial governance, allowing the group to accurately monitor staffing costs and ensure the financial stability of all schools within the group.

**Lawful Basis:** We process this data under UK GDPR Article 6(1)(f) – Legitimate Interests. We have conducted a Legitimate Interests Assessment (LIA) which concludes that this

administrative sharing is necessary for group financial management and is conducted in a way that is professional and proportionate.

**International transfers:** Galaxy Global Education Ltd is registered in the UK and processes shared data within the UK. Should any data be transferred outside the UK in future, appropriate safeguards will be put in place under the International Data Transfer Agreement (IDTA) or equivalent mechanism, and this policy will be updated accordingly.

Safeguards and Restrictions:

- No HR Impact: This data is explicitly forbidden from being used for HR, performance management, or disciplinary purposes.
- Strict Access: Access is restricted to specific authorised roles within the group finance function (such as the Group Bursar) under a "Least Privilege" principle.
- Security: All shared data is protected by encryption and is subject to a formal Data Sharing Agreement between the School and the parent company.
- Your Rights: You retain all your rights under UK GDPR, including the right to object to this processing on grounds relating to your particular situation. The School will cease such processing unless it can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms. For more information on how to exercise your rights, please contact the Data Protection Officer.

The Legitimate Interests Assessment is available on request or held by the Data Protection Officer.

## 5. Headline responsibilities of all staff

## Record-keeping

These responsibilities apply equally to all staff in relation to data about pupils, colleagues, parents, governors, contractors, and any other individuals whose data they access in the course of their work.

All personal data held by the School must be accurate, fair, and sufficient for its intended purpose. Staff are required to notify the School if they believe that any personal data about themselves or others is inaccurate, outdated, or incomplete.

When recording personal data about colleagues (including line management notes, HR-related observations, or professional correspondence), pupils, or parents, staff must ensure that records are professional, precise, and appropriate. Individuals may have rights to access the information recorded about them; however, staff must continue to make necessary and accurate records of incidents or conversations in line with other School policies. Where legally justified, access may be restricted. Staff should assume that any record could be viewed by the individual it concerns and maintain it to a standard they could confidently stand by.

All staff must complete mandatory data protection training during induction and refresher training at least annually. Completion is recorded by HR and forms part of the School's compliance records.

## Data handling

Staff must handle all personal data they access in a lawful, fair, responsible, and secure manner, in line with School policies and procedures. Data protection considerations apply across multiple areas of School activity, including safeguarding, pastoral care, and IT security. This includes staff personal data accessed through HR systems, safeguarding referrals involving staff, performance management information, and occupational health data. Staff must read and comply with:

- Taking, Storing, & Using Images of Pupils Policy
- CCTV Policy
- Record Keeping Policy
- Safeguarding, Pastoral, and Health & Safety Policies, including procedures for incident reporting
- IT Policies, including Acceptable Use and E-Safety Policies

The obligation to process personal data responsibly also applies when creating new records. All such processing must be lawful, secure, and compliant with UK GDPR and the Data Protection Act 2018.

## Avoiding, mitigating and reporting data breaches

UK GDPR and the Data Protection Act 2018 require that personal data breaches which may affect individuals be reported promptly. The School must notify the ICO within 72 hours (Article 33 UK GDPR) if a breach risks impacting individuals' rights and freedoms. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the School will also notify affected individuals without undue delay (Article 34 UK GDPR).

Staff must immediately inform the Data Protection Officer if they become aware of any personal data breach. Even minor breaches must be reported so that the School can assess their impact and take remedial action. Staff uncertain about reporting should always err on the side of caution.

Failure to report a breach may expose the School and affected individuals to harm and could result in disciplinary action, regardless of whether the breach was intentional or accidental.

The Data Protection Officer maintains a Data Breach Register recording all incidents, including minor breaches and near misses, with actions taken and lessons learned.

This applies equally to breaches involving staff personal data, including HR files, payroll data, or internal investigations.

## Care and data security

All staff must be aware of the data protection principles, attend mandatory training, and ensure compliance whenever they process personal data. Induction training and periodic refresher courses are required, as determined by the Data Protection Officer. Data security applies to both digital and physical formats, including filing and sending correspondence. Staff must always use secure delivery methods and consider the consequences of potential loss or unauthorised access.

Managers and leaders are expected to model good data protection practices, ensure timely reporting of concerns to the Data Protection Officer, and implement ongoing training for their teams to maintain awareness and compliance.

This includes safeguarding confidentiality of staff HR records, disciplinary documentation, and any employee-related sensitive data.

## 6. Rights of Individuals

Individuals whose data is processed by the School have specific rights under UK GDPR and the Data Protection Act 2018. Chief among these is the right to access their personal data, known as a 'subject access request' (SAR). SARs must be handled promptly, without formalities, and typically responded to within one month of receipt unless an extension is legally justified. Staff

must immediately inform the Data Protection Officer if they receive any SAR or other communication regarding an individual's data rights. These rights apply equally to staff members in relation to their employment and HR records held by the School.

Individuals also have the right to:

- Request correction of inaccurate personal data
- Request deletion of personal data in certain circumstances
- Request restriction of processing in specific circumstances
- Receive their data in a commonly used format to transmit to another controller (data portability)
- Object to processing based on legitimate interests (Article 6(1)(f) UK GDPR) on grounds relating to their particular situation — the School will cease such processing unless it can demonstrate compelling legitimate grounds that override the individual's interests, rights, and freedoms
- Object to automated decision-making, including profiling, and withdraw consent where consent was relied upon as the lawful basis

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk if they believe their personal data has been processed unlawfully (Article 77 UK GDPR).

Except for withdrawal of consent, these rights are subject to legal exceptions. Any requests relating to an individual's data rights must be referred to the Data Protection Officer immediately.

Before responding to any data rights request, the School will verify the requester's identity to ensure that personal data is only disclosed to authorised individuals. For complex or numerous requests, the School may extend the response period by up to two months, in accordance with Article 12(3) UK GDPR, with the Data Protection Officer providing an explanation of the extension to the requester.

## 7. Data Security: online and digital

The School must maintain strict security measures to protect personal data from unauthorised access, accidental loss, or damage. Staff are not allowed to remove personal data — which includes staff HR records, payroll data, safeguarding records involving staff, and any internal employment documentation, digital or physical — from School premises without prior consent from the Head or an appropriate SLT member. Any approved off-site data must be encrypted; encrypted storage devices can be obtained from the Data Protection Officer. The use of personal email accounts or unencrypted personal devices for School business is strictly prohibited.

The School implements multi-factor authentication (MFA) and endpoint protection on all staff devices and systems handling personal data. All paper and digital records are securely disposed of once retention periods expire, using approved methods such as certified shredding and secure data wiping in accordance with the Data Retention Policy.

## 8. Processing of Credit Card Data

The School adheres to the PCI Data Security Standard (PCI DSS) for processing credit card information. Staff handling credit card data must follow the current PCI DSS requirements. If unsure about compliance, staff should consult the Bursar or DPO for guidance.

## 9. Summary

Effective data protection is essential for everyone at Plymouth College. Staff must handle all personal data fairly, lawfully, securely, and responsibly. This includes the protection of both pupil and staff personal data across all operational areas of the School.

When processing data, ask yourself:

- Would I be comfortable if this personal information were shared as intended?
- Could I confidently stand by my record if the individual could see it?
- What are the potential consequences of misplacing or misdirecting this data?

Data protection is not merely regulatory compliance; it is a set of practical principles to guide how we handle personal information, maintain trust, and strengthen relationships. All staff and representatives are expected to integrate these practices into their daily work and the School culture.