PLYMOUTH COLLEGE

DATA PROTECTION POLICY

Including Early Years Foundation Stage

Last reviewed:	**October 2025**
Next review date:	**May 2026**
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, including sensitive 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.

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. More recently, the Data Use and Access Act 2025 (DUAA 2025) provides additional statutory duties and safeguards for the processing of personal data in UK independent schools. 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, but the School also has obligations under DUAA 2025, which strengthen accountability, record-keeping, and data access controls. 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, including DUAA 2025.

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, DPA 2018, and DUAA 2025.

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 is the Controller of pupils' personal information. As a Data Controller, 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.
- **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. 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.

2. Data Privacy Officer

The School has appointed Mr James Moate as the Data Privacy Officer, who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the 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 Privacy Officer at privacy@plymouthcollege.com in the first instance.

3. The Principles

The GDPR, DPA 2018, and DUAA 2025 set out six core principles for the lawful processing of personal data. All data controllers and processors must ensure that personal data is:

1. Processed lawfully, fairly, and transparently;
2. Collected for specified, explicit purposes and not used beyond those purposes;
3. Adequate, relevant, and limited to what is necessary for the intended purpose;
4. Accurate and kept up to date;
5. Retained no longer than necessary for the purpose for which it was collected; and
6. Secured appropriately to prevent unauthorised or unlawful processing, loss, or damage.
7. Integrity and confidentiality underpin all the above and require 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 DPO.

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;
- 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 GDPR, DPA 2018, and DUAA 2025.

4. Lawful grounds for data processing

Under GDPR, DPA 2018, and DUAA 2025, personal data may only be processed if there is a lawful basis. Consent is one such basis, but it must be explicit, informed, and revocable, making other grounds preferable where feasible.

A common lawful basis is 'legitimate interests', which requires careful balancing between the rights of the individual and the interests of the School. Data subjects have the right to challenge the School's legitimate interest processing, so transparency and proper assessment are mandatory. 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;
- 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 GDPR, DPA 2018, and DUAA 2025.

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 and the provisions of DUAA 2025.
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 DPO 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 and DUAA 2025 to identify and mitigate risks. The School maintains a standard DPIA template approved by the

DPO. A DPIA must be completed before any new high-risk system, vendor, or processing activity begins.

5. Headline responsibilities of all staff

Record-keeping

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, 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. 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 GDPR, DPA 2018, and DUAA 2025.

Avoiding, mitigating and reporting data breaches

GDPR, DPA 2018, and DUAA 2025 require that personal data breaches which may affect individuals be reported promptly. The School must notify the ICO within 72 hours if a breach risks impacting individuals' rights and freedoms.

Staff must immediately inform the Data Privacy 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 DPO maintains a Data Breach Register recording all incidents, including minor breaches and near misses, with actions taken and lessons learned. 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.

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 DPO. 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 DPO, and implement ongoing training for their teams to maintain awareness and compliance.

6. Rights of Individuals

Individuals whose data is processed by the School have specific rights under 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 DPO if they receive any SAR or other communication regarding an individual's data rights.
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
- Object to certain processing activities if it disproportionately affects them
- Object to automated decision-making, including profiling, and withdraw consent where relied upon.

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 DPO 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 DPO 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—digital or

physical—from School premises without prior consent from the Head or an appropriate SLT member. Any approved offsite data must be encrypted; encrypted storage devices can be obtained from the DPO. 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.
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.