DATA PROTECTION POLICY

Including Early Years Foundation Stage

Last reviewed:	**April 2024**
Next review date:	**April 2026**
Responsibility:	**Head of Systems & IT, DPO**
Governance:	**Finance & General Purpose Committee**

1. Background

Data protection is an important legal compliance issue for Plymouth College ("the School"). During the course of the School's activities, it collects, stores and processes personal data (sometimes sensitive) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the School's Privacy Notice). It is, therefore, an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data is sensitive or routine.

The existing law (Data Protection Act 1998) changed on 25th May 2018 with the implementation of the General Data Protection Regulation (**GDPR**). This EU Regulation is directly effective in the UK and throughout the rest of Europe. A new Data Protection Act 2018 has also been passed to deal with certain issues left for national law: this includes specific provisions of relevance to independent schools. In particular, in the context of our safeguarding obligations, the School has a heightened duty to ensure that pupils' personal data is at all times handled responsibly and securely.

While this new law does set out useful legal grounds in this area, it mostly strengthens the rights of individuals and places tougher compliance obligations on organisations that handle personal information, including schools. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law and has powers to take action for breaches of the law.

Those who process personal data are obliged to comply with this policy. Accidental breaches will happen and may not be a disciplinary issue, but any breach of this policy may result in disciplinary action. This policy may be amended at any time.

This policy sets out the school's expectations and procedures with respect to processing any personal data we collect from data subjects (e.g., parents, carers, guardians, pupils, and employees).

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.

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 sets out six principles relating to the processing of personal data, which must be adhered to by data controllers (and data 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 used 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.

The GDPR's 'accountability' principle also requires that the School not only processes personal data fairly and legally but can also *demonstrate* that its processing is lawful. This involves, among other things:

- keeping records of its data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how it uses personal data; 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;
    - any breaches have been dealt with, etc.

4. Lawful grounds for data processing

Under the GDPR, several different lawful grounds exist for processing personal data. One of these is consent. However, because the definition of what constitutes consent has been tightened under GDPR (and consent can be withdrawn by the data subject), it is generally considered preferable to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', 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 Controller. Data subjects can challenge it, meaning the Controller 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 GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents;
- A narrower set of grounds for processing special categories of personal data (such as health information) that includes explicit consent, emergencies, and specific public interest grounds.

5. Headline responsibilities of all staff

Record-keeping

It is important that the personal data held by the School is accurate, fair, and adequate. You are required to inform the School if you believe that your personal data is inaccurate or untrue or if you are dissatisfied with the information in any way. Similarly, it is vital that the way you record the personal data of others, in particular, colleagues, pupils, and their parents, is accurate, professional, and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information in emails and notes on School business may have the right to see that information. This absolutely must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils in accordance with the School's other policies, and grounds may exist to withhold these from such requests. However, the starting position is to record every document or email so that you could stand by it if the person about whom it was recorded were to see it.

Data handling

All staff are responsible for handling the personal data they come into contact with fairly, lawfully, responsibly, and securely in accordance with all relevant school policies and procedures. In particular, there are data protection implications across several areas of the School's wider responsibilities, such as safeguarding and IT security, so all staff should read and comply with the following policies:

- the School's policy on Taking, Storing, & Using Images of Pupils;
- the School's CCTV Policy;
- the School's Record Keeping Policy;
- the School's safeguarding, pastoral, and health and safety policies, including procedures for recording concerns or incidents; and
- the School's IT policies, including its Acceptable Use Policy and E-Safety Policy.

Responsible processing also extends to creating and generating new personal data/records, which should always be done fairly, lawfully, responsibly and securely.

Avoiding, mitigating and reporting data breaches

One key new obligation in the GDPR is reporting personal data breaches. Data Controllers must report certain types of personal data breaches (those that risk an impact on individuals) to the ICO within 72 hours.

In addition, Data 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 you become aware of a personal data breach, you must notify the Data Privacy Officer. If staff are in any doubt as to whether or not you should report something, it is always best to do so. A personal data breach may be serious or minor, and it may involve fault or not, but the School always needs to know about it to decide.

As stated above, the School may not need to treat the incident as a disciplinary matter, but failing to report it could result in significant exposure for the School and those affected and could be a serious disciplinary matter, whether under this Policy or the staff member's contract.

Care and data security

More generally, Plymouth College requires all School staff to remain conscious of the data protection principles (see section 3 above), attend any required training, and 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 affects daily processes: filing and sending correspondence, notably hard copy documents. Staff should always consider the most assured and secure means of delivery and the consequences of loss or unauthorised access.

Plymouth College expects all those with management/leadership responsibilities to champion these principles, oversee the swift reporting of any concerns about how personal information is used by the School to the Data Privacy Officer, and identify the need for (and implement) regular staff training.

6. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain rights, perhaps most significantly that of access to their personal data held by a Data Controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests' - SAR). Such a request must be dealt with promptly and does not need any formality or to refer to the correct legislation. If you become aware of a subject access request (or any communication from an individual about their personal data), you must tell the School's DPO 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 to transmit it in a commonly used format to another data controller;
- 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, and
- object to automated individual decision-making, including profiling (where a significant decision is made about the individual without human intervention), and to direct marketing, or to withdraw their consent where we rely on it to process their personal data.

Except for the final bullet point, none of these individual rights are unqualified, and exceptions may apply. In any event, however, if you receive a request from an individual purporting to exercise one or more of their data protection rights, you must tell Mr Moate as soon as possible.

7. Data Security: online and digital

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data and the accidental loss of, or damage to, personal data. As such, no staff member is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without the Head's prior consent or an appropriate Senior Leadership Team member. Where a worker is permitted to take data offsite, it will need to be encrypted, and encrypted data sticks are available from the Data Privacy Officer for this purpose. Using personal email accounts or unencrypted personal devices for official School business is prohibited.

8. Processing of Credit Card Data

The School complies with the PCI Data Security Standard (PCI DSS) requirements. Staff required to process credit card data must ensure they know and comply with the most up-to-date PCI DSS requirements. If unsure, please seek further guidance from the Bursar or DPO.

9. Summary

It is in everyone's interest to get data protection right and think carefully about data protection issues. This means handling all personal information with which you come into contact fairly, lawfully, securely, and responsibly.

A good rule of thumb here is to ask yourself questions such as:

- Would I be happy if my personal information were being used (for example, shared with a third party) in the way I propose? Would I expect it?
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned could see it?
- What would be the consequences of my losing or misdirecting this personal data?

Data protection law is, therefore, best seen not as oppressive red tape or a reason not to do something necessary or important but as a code of useful and sensible checks and balances to improve how we handle and record personal information and manage our relationships with people. This is an important part of the School’s culture, and all its staff and representatives must be mindful of it.