DATA PROTECTION POLICY

Policy Owner PPS Director of Operations and Finance	**Applies to** Prior Park Schools (Trust Wide)	**Superseded documents** PPS Data Protection Policy v2
Associated documents Privacy Notice(s) Retention and Destruction Handbook Policy Data Processing Agreement Data Protection Impact Assessment(s) Annual Review of School Records Document Data Subject Handling Procedure Intellectual Property Policy Cyber Incident Response Policy	**Review frequency** Every year (unless the legislation/regulations update before this time) **Implementation date** 31 March 2022	**Legal Framework** UK General Data Protection Regulations (UK GDPR) Data Protection Act (DPA) 2018 ICO Guidance

This policy is reviewed annually, or more regularly as required, prior to approval by Trustees, where applicable.

Last reviewed by:	Head of Compliance (Emma Wickham), ICT Manager (Andy Haines) and Director of Operations and Finance (Emma Sandberg)
Date last reviewed:	February 2022
Approved by Trustees:	Board of Trustees
Date last approved:	31 March 2022
Date for next approval:	March 2023

1. Introduction

Prior Park Schools (PPS) comprises three schools. Two of those schools, Prior Park College (PPC) and The Paragon School (TP) are incorporated in England as Prior Park Educational Trust Ltd. The third school, Prior Park School Gibraltar (PPSG), is incorporated in Gibraltar as Prior Park School Ltd. Both are companies limited by guarantee and registered charities.

2. Background

The UK left the EU on 31 January 2020 and entered a transition period, which ended on 31 December 2020. This Policy has been updated to reflect the current position. We will keep this under review and update it as the situation evolves.

Data protection is an important compliance issue for PPS.

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (**EU GDPR**) – an EU Regulation that is directly effective in the UK, and the new Data Protection Act 2018 (**DPA 2018**) was also passed to deal with certain issues left for national law.

The DPA 2018 included specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to Personal Data.

The provisions of the EU GDPR were incorporated directly into UK law at the end of the Brexit transition period becoming the UK GDPR. The UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK-only context. At present the same aspects of the UK GDPR are incorporated in Gibraltar.

Without fundamentally changing the principles of data protection law, and while providing some helpful new grounds for processing certain types of Personal Data, in most ways this new law has strengthened the rights of individuals and increased the compliance obligations of PPS . The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

For PPSG specifically: This policy is written with specific reference to the information and guidance on the conditions for consent under the Data Protection Act 2004 ("DPA") and the EU General Data Protection Regulation 2016/679 ("GDPR"). It's important to note that the concept of consent is not new, as its definition and role remains similar to that under the previous EU Data Protection Directive 95/46/EC and the current ePrivacy Directive 2002/58/EC (the "ePrivacy Directive").

Details of the processing of data can be found in the entry in the ICO Register of Data Controllers (no: Z6476375) and Gibraltar Regulatory Authority.

During the course of our activities we collect, store and process Personal Data (sometimes sensitive in nature) about staff, students, their parents, alumni, contractors and other third parties (in a manner fully detailed in the appropriate PPS Privacy Notice(s)).

PPS, as "Data Controller", is liable for the actions of our staff and trustees in how they handle data. It is therefore an area where all staff and trustees have a part to play in ensuring we comply with our legal obligations.

All PPS staff and trustees that have access to **Personal Data** will have their responsibilities under this policy outlined to them as part of their induction training. In addition, each school will provide annual Data Protection training and procedural guidance for their staff.

PPS Leadership Teams and trustees are fully committed to ensuring continued and effective implementation of this policy and expect all PPS staff and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

This policy applies to all PPS staff and trustees and all Third Parties responsible for the processing or handling of Personal Data on behalf of PPS.

This policy sets forth the expected behaviours of all PPS staff and trustees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a PPS contact (i.e. the **Data Subject**)

For the purposes of this policy, any reference to:

- staff relates to all past and current employed, voluntary and agency personnel.
- student relates to past, current and prospective students.
- parent relates to past, current and prospective parents.

3. Definitions

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

- **Data Subject -** The identified or identifiable living individual to whom Personal Data relates
- **Third Parties -** those who handle PPS Personal Data as contractors, whether they are acting as "Data Processors" on our behalf (in which case they will be subject to binding contractual terms) or as Data Controllers responsible for handling such Personal Data in their own right (Third Party Data Controllers). Where we share Personal Data with Third Party Data Controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – each party will need a lawful basis to process that Personal Data, and will be expected to do so lawfully and with due regard to security and confidentiality, as per UK GDPR and DPA 2018.
- **Data Controller** – a person or body that determines the purpose and means of the processing of Personal Data, and who is legally responsible for how it is used. For example, the School (including by its trustees) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a Data Controller.
- **Data Processor** – an organisation that processes Personal Data on behalf of a Data Controller, for example a payroll or IT provider or other supplier of services with whom

Personal Data may be shared but who is not authorised to make any decisions about how it is used.

- **Personal Data Breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
- **Personal Data -** any information relating to a living individual (a Data Subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). the definition includes expressions of opinion about the individual or any indication of the school's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with Personal Data, 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.
- **Subject Access Request (SAR)** - individuals have the right to ask PPS whether or not they are using or storing their personal information. Individuals can also ask PPS for copies of their personal information, verbally or in writing. This is called the right of access and is commonly known as making a Subject Access Request 'SAR'. (Further information can be found in the PPS Data Subject Handling Procedure).
- **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, genetic or biometric data used to identify an individual. There are also separate rules for the processing of Personal Data relating to criminal convictions and offences (please see our Appropriate Policy Document for further guidance)

4. Application of this Policy

Those who handle Personal Data as staff or trustees of PPS are obliged to comply with this policy when doing so. For staff, breaches of this policy may result in disciplinary action.

Accidental breaches of the law or this policy in handling Personal Data will happen from time to time, for example by human error, and will not always be treated a disciplinary issue. However, failure to report breaches that pose significant risks to PPS, the school or individuals will be considered a serious matter.

5. Person Responsible for Data Protection across PPS

PPS has appointed the Director of Operations and Finance (DOF) as the Data Protection Controller who will endeavour to ensure that all Personal Data is processed in compliance with this Policy and the principles of the UK GDPR. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Prior Park Schools Head of Compliance (HoC), who acts as the nominated person with responsibility for Data Protection processes.

The Data Protection Controller and the HoC will inform and advise PPS and its staff and trustees who carry out processing pursuant to Data Protection regulations, national law or union-based Data Protection provisions;

- Ensuring the alignment of this policy with Data Protection regulations, national law or union-based Data Protection provisions
- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs)

- Acting as a point of contact for and cooperating with Data Protection Authorities
- Determining the need for notifications to one or more Data Protection Authorities as a result of PPS current or intended Personal Data processing activities
- Making and keeping current notifications to one or more Data Protection Authorities as a result of PPS current or intended Personal Data processing activities
- The establishment and operation of a system providing prompt and appropriate responses to Subject Access Requests
- Informing senior leaders and managers, and trustees of PPS of any potential corporate, civil and criminal penalties which may be levied against PPS and/or its staff and/or its trustees for violation of applicable Data Protection laws.

Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this policy by any:

- provides Personal Data to PPS
- receives Personal Data from PPS
- has access to Personal Data collected or processed by PPS

6. Data Protection Principles

The UK 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 only for the purposes it was collected for
3. **Relevant** and **limited** to what is necessary for the purposes it is processed for
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 UK GDPR's broader 'accountability' principle also requires that PPS not only processes Personal Data in a fair and legal manner but that we are also able to *demonstrate* that our processing is lawful.

This involves, among other things:

- keeping records of our Data Processing activities, including by way of logs and policies
- documenting significant decisions and assessments about how we use Personal Data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis Data Protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any Data Protection consents were collected from individuals; how Personal Data breaches were dealt with, whether or not reported (and to whom), etc.

7. Lawful grounds for Data Processing

Under the UK GDPR there are several different lawful grounds for processing Personal Data. One of these is consent. However, because the definition of what constitutes consent has been tightened under the UK GDPR (and the fact that it can be withdrawn by the Data Subject) it is considered preferable for PPS to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is 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 PPS. It can be challenged by data subjects and also means

PPs is taking on extra responsibility for considering and protecting people's rights and interests. PPS' legitimate interests are set out in its Privacy Notice, as UK GDPR requires.

Staff and trustees should discuss with the Director of Operations and Finance and/or the Assistant Head Compliance before processing data via legitimate interest or one of the other lawful grounds as stated below.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity
- contractual necessity, e.g. to perform a contract with staff, trustees or parents, or the engagement of contractors
- a narrower set of grounds for processing Special Categories of Personal Data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

8. Headline responsibilities for all staff

a. Record-keeping

It is important that Personal Data held by PPS and the individual school is accurate, fair and adequate. Staff and trustees are required to inform the school if they believe that *any* Personal Data is inaccurate or untrue or if they are dissatisfied with how it is recorded. This applies to how staff record their own data, and the Personal Data of others – in particular colleagues, students and their parents – in a way that is professional and appropriate.

Staff and trustees should be aware of the rights set out below, whereby any individuals about whom they record information on school business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff or trustees from recording necessary and sometimes difficult records of incidents or conversations involving colleagues or students, in accordance with the school's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff and trustees is to **record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it**.

b. Data handling

All staff and trustees have a responsibility to handle the Personal Data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the individual school staff handbook(s) and all relevant school policies and procedures (to the extent applicable to them).

In particular, there are data protection implications across a number of areas of the school's wider responsibilities such as safeguarding and IT security, so all staff and trustees should read and comply with the following policies:

I. Safeguarding Policy
II. E-Safety Policy
III. ICT Systems Policy
IV. Privacy Notice(s)
V. Taking, storing and using student images Policy
VI. Staff Code of Conduct Policy
VII. Policy for the Processing of Special Category Data
VIII. Cyber Incident Response Policy

Responsible processing also extends to the creation and generation of new Personal Data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

c. Avoiding, mitigating and reporting Data breaches
One of the key new obligations contained in the UK GDPR is on reporting Personal Data breaches. The Data Protection Controller at UK schools must report certain types of Personal Data breach (those which risk an impact to individuals) to the ICO within 72 hours.
Likewise, the Data Protection Controller will ensure all Personal Data breaches made in PPSG are reported (where applicable) to the Information Rights Division, Gibraltar Regulatory Authority 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, PPS must keep a record of any Personal Data breaches, regardless of whether we need to notify the ICO. If staff become aware of a Personal Data breach, they must notify the DOF and the HoC immediately. If staff are in any doubt as to whether to report something internally, it is always best to do so. A Personal Data breach may be serious, or it may be minor; and it may involve fault or not; but PPS always needs to know about them to make a decision.

As stated above, PPS may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for PPS and/or the individual school, and for those affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

d. Data security
More generally, we require all staff and trustees (and expect all our contractors) to remain mindful of the Data Protection principles (see section 4 above), and to use their best efforts to comply with those principles whenever they process Personal Data.

Data security is not simply an online or digital issue but one that affects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how Personal Data is used by PPS, and to identity the need for (and implement) regular staff training. Staff and trustees must attend any training we require them to.

9. Rights of Individuals

In addition to PPS' responsibilities when processing Personal Data, individuals have certain specific rights, perhaps most significantly that of access to their Personal Data held by a Data Controller (i.e. PPS and/or the individual school). This is known as the 'subject access right' (or the right to make 'subject access requests' (SARs – as defined in section 3). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation. If you become aware of a Subject Access Request (or indeed any communication from an individual about their Personal Data), you must tell the DOF and the HoC 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 for the purpose of transmitting 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.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention)
- object to direct marketing; and
- withdraw one's consent where we are relying on it for processing their Personal Data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their Data Protection rights, you must tell the DOF and the HoC as soon as possible.

Data Subjects with a complaint about the processing of their Personal Data, should put forward the matter in writing to the Data Protection Controller. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Controller will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Controller, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction. (Please see our Complaints Policy or contact the ICO directly https://ico.org.uk/ for UK schools or the Gibraltar Regulatory Authority for PPSG).

10. Data Collection

a. Consent

Each school will obtain Personal Data only by lawful and fair means and where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their Personal Data, we are committed to seeking such consent. The Data Protection Controller, in cooperation with other relevant representatives, shall establish a system for obtaining and documenting Data Subject consent for the collection, processing, and/or transfer of their Personal Data.

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be notified unless one of the following apply:

  - The Data Subject has received the required information by other means.
  - The information must remain confidential due to a professional secrecy obligation
  - A national law expressly provides for the collection, processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Data
- At the time of first communication if used for communication with the Data Subject
- At the time of disclosure if disclosed to another recipient.

b. Protection
Each school will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to Data Processing systems in which Personal Data are processed.
- Prevent persons entitled to use a Data Processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a Data Processing system.
- Ensure that in the case where processing is carried out by a Data Processor, the data can be processed only in accordance with the instructions of the Data Controller.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is processed separately.
- Ensure that Personal Data is not kept longer than necessary

c. Retention
To ensure fair processing, Personal Data will not be retained by PPS for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which we need to retain Personal Data is set out in our 'Retention and Destruction Handbook Policy'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

11. Subject Access Requests (SAR)

The Data Protection Controller will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure. If an individual makes a request relating to any of the rights listed above

We will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a

request unless the request is deemed to be unnecessary or excessive in nature. Data Subjects can make a request via any member of staff, verbally or in writing (including email) or by completing the Subject Data Access Request form and send it to;

Prior Park Educational Trust
Data Protection Controller (Director of Operations and Finance)
Prior Park College
Ralph Allen Drive
Bath
BA2 5AH

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that other person's rights. Detailed guidance for dealing with requests from Data Subjects can be found in our 'Data Subject Handling Procedures' document.

If any staff receive a SAR they must inform the Director of Operations and Finance and Head of Compliance immediately.

12. Compliance Monitoring

To confirm that an adequate level of compliance that is being achieved by all schools in relation to this policy, the Data Protection Controller (or their appointed nominee) will carry out an annual Data Protection Annual Review of School Records.

13. Special Categories of Data

We will only process Special Categories of Data (also known as sensitive data) where we have identified a lawful basis under Article 6 and a condition for processing Article 9 of the UK GDPR.

The UK GDPR defines special category data as:

- Personal Data revealing **racial or ethnic origin**
- Personal Data revealing **political opinions**
- Personal Data revealing **religious or philosophical beliefs**
- Personal Data revealing **trade union membership**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

This does not include Personal Data about criminal allegations, proceedings or convictions, as separate rules apply (Please see our Policy for the Processing of Special Category Data).

We must always ensure that our processing is generally lawful, fair and transparent and complies with all the other principles and requirements of the UK GDPR. To ensure that our processing is lawful, we need to identify an Article 6 basis for processing.

Processing shall be lawful only if and to the extent that at least one of the following applies:

1. the Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes

2. processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract
3. processing is necessary for compliance with a legal obligation to which the Data Controller is subject
4. processing is necessary in order to protect the vital interests of the Data Subject or of another natural person
5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller
6. processing is necessary for the purposes of the legitimate interests pursued by the data Controller or by a Third Party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

In addition, PPS can only process Special Category Data if one of the specific conditions in Article 9 of the UK GDPR is met.

Article 9 lists the conditions for processing Special Category Data:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

a. Children's Data

Children under the age of 13 are unable to consent to the processing of Personal Data. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

b. Digital Marketing

The Privacy and Electronic Communications Regulations (PECR) sit alongside the DPA 2018 the UK GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure; and
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

PPC and TP aim to comply with PECR. This means that when we send electronic marketing or use cookies or similar technologies, we comply with both PECR, DPA 2018 and the UK GDPR.

PPSG will continue to comply with the guidance on the ePrivacy Regulation, and whilst we aware that it is currently under review, this policy will be updated once the position is clearer. In the interim, if in doubt PPSG staff should ask the Director of Operations and Finance or the Assistant Head Compliance.

PPS will not send promotional or direct marketing material to a contact through digital channels such as mobile phones, email and the Internet, without first obtaining their consent. Any school wishing to carry out a digital marketing campaign cannot do so without obtaining prior consent from the Data Subject. Where personal data processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data processed for such purposes.

If the Data Subject puts forward an objection, digital marketing related processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted. It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

Each external website provided by PPS will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

c. Data Protection by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing. Each school will ensure that a Data Protection Impact Assessment (DPIA) is conducted, in cooperation with the Data Protection Controller, for all new and/or revised systems or processes for which it has responsibility.

Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the Data Protection Controller to assess the impact of any new technology uses on the security of Personal Data.

d. Prior Park Alumni

Prior Park Alumni (PPA) has a website forum for former students, staff, parents and friends of PPS. Every individual is specifically asked if they give consent and must therefore 'opt in' to the PPA.

Occasionally the Prior Park Alumni will receive a request for names of past students in a particular year group. PPA will, if for legitimate reasons, disclose this information, which can be used independently by the enquirer to search for further details on social media sites. PPA will not disclose contact information (phone, mobile, email, postal address).

On request, PPA may assist by publishing a message in the Gossip Bowl (Annual Alumni magazine) with the enquirer's contact details. Where the request relates to only a few past students the PPA will usually send an e-mail to each of them informing them of the request and providing them with the enquirer's details should they wish to make contact. Where there is no e-mail address on the database, PPA may consider it appropriate to telephone them.

PPS Development Office uses a Third Party provider outside of the EEA. Data Transfers are made in compliance with the DPA and GDPR.

14. Data Transfers

PPS may transfer Personal Data to internal or third party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant Data Subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in

compliance with our approved transfer mechanism, as stated below. PPS may only transfer Personal Data where one of the transfer scenarios listed below applies:

- The Data Subject has given consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject

a. Transfers between Prior Park Schools
In order for PPS to carry out its operations effectively across its various schools, there may be occasions when it is necessary to transfer Personal Data internally from one school to another, or to allow access to the Personal Data from an overseas location. Should this occur, the school sending the Personal Data remains responsible for ensuring protection for that Personal Data. Transfers between the schools should only be made through internal means; either via school email accounts or through a shared folder (e.g. OneDrive, SharePoint or Teams).

Additionally, PPS transfer Personal Data to individual parents and/or guardians, and on occasion in group correspondence. All staff must use the approved system for doing this e.g. SchoolBase (Staff should ensure they have read the Staff IT Code of Conduct)

b. Transfers to Third Parties
Each school will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third Party (as defined in section 3) processing takes place, each school will first identify if, under applicable law, the Third Party is considered a Data Controller, or a Data Processor of the Personal Data being transferred. Where the Third Party is another School, University or Agent all emails should be sent using an Encrypted Email transfer/or Share Folders (please see the Staff IT Code of Conduct)

Data Controller e.g. Prior Park Schools

- to collect the Personal Data and has the legal basis for doing so
- which items of Personal Data to collect
- to modify the data
- the purpose or purposes the data are to be used for
- whether to share the data, and if so, with whom
- how long to retain the data

Data Processor e.g. School MIS

- implement IT systems or other methods to collect Personal Data
- use certain tools or techniques to collect Personal Data
- install the security surrounding the Personal Data
- store the Personal Data

Where the Third Party is deemed to be a Data Controller, PPS will enter into an appropriate agreement with the Data Controller to clarify each party's responsibilities in respect to the Personal Data transferred. Where the Third Party is deemed to be a Data Processor, PPS will enter into, an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only

process Personal Data in compliance with PPS instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

PPS has a 'Data Processing Agreement' document that should be used when a school is outsourcing services to a Third Party. This will identify whether the Third Party will process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include adequate provisions in the outsourcing agreement for such processing and Third Country transfers.

c. Transfer outside of the EEA

Personal Data is held in the UK on secure servers by approved contractors. Any transfers of Personal Data overseas (outside of the European Economic Area), for example to an international agent, are protected either by a European Commission 'adequacy decision' (declaring the recipient country as a 'safe' territory for Personal Data) or by standard contractual clauses adopted by the European Commission, which obligate the recipient to safeguard the Personal Data. Where the Third Party is outside of the EEA data can be sent through an Encrypted Email transfer/or Share Folders.

Further information about the measures we use to protect Personal Data when being transferred internationally is available from our Data Protection Controller.

15. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of a safeguarding risk.
- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If PPS processes Personal Data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If PPS receives a request from a court or any regulatory or law enforcement authority for information relating to a PPS contact, you must immediately notify the Data Protection Controller who will provide comprehensive guidance and assistance.