

*This School is committed to ensuring the best possible environment for the children and young people in its care. Safeguarding and promoting the welfare of children and young people is our highest priority.*



**PARKSIDE**  
SCHOOL

## DATA PROTECTION POLICY

This policy is applicable to the whole school, including the Early Years Foundation Stage (EYFS)

**Edition: 16 June 2021**

### Policy owner

DRW

### Monitoring, Evaluation and Review

This Policy is monitored, evaluated and reviewed on a biennial basis by the Senior Leadership Team.

Review	Date	Detail	Reviewer	Agreed
9	10.6.21	Governors' review	F&R Cttee	16.6.21
8	1.6.21	SLT biennial review	SLT	9.6.21
7	1.3.20	Governors' annual review	F&R Cttee	3.3.20
6	24.2.20	SLT Annual review	SLT	27.2.20
5	1.3.19	Governors' annual review	F&R Committee	7.3.19
4	21.2.19	SLT Annual review	SLT	28.2.19
3	18.6.18	All Governors' review	Board of Governors	25.6.18
2	4.6.18	Governors' first review	F&R Committee	11.6.18
1	24.5.18	New Policy – SLT initial review	SLT	25.5.18

### References:

Keeping Children Safe in Education (January 2021) (**KCSIE**)

ISI: Commentary on the Regulatory Requirements 2020-09 (September 2020)

Working Together to Safeguard Children (August 2018) (**WT**)

Data Protection Act (May 2018) (**DPA**)

General Data Protection Regulation (May 2018) (**GDPR**)

Statutory Framework for the Early Years Foundation Stage (Childcare Act 2006) (revised April 2017)

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/>

## **1. Introduction**

Parkside School (the School) is committed to providing the best possible care and education to its pupils and to safeguarding and promoting the welfare of children and young people.

## **2. Scope of this Policy**

Data protection is an important legal compliance issue for the School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, suppliers and other third parties (in a manner more fully detailed in the School's Privacy Notices. The School, as "data controller", is liable for the actions of its staff and governors in how they handle data. 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.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). The DPA 2018 includes 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.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office (ICO) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

## **3. Aims**

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, 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 as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's 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.

Where the School shares 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 set out in this policy.

### **Links to other policies**

- CCTV Policy
- Bring Your Own Device (BYOD) Policy
- Data Breach Management Policy
- E-Safety Policy
- Health & Safety policies
- IT Acceptable Use Policy
- Mobile Phone policies (including EYFS)
- Parent Contract (Terms and Conditions)
- Privacy Notices
- Remote Learning Policy
- Remote Working: Access & Devices
- Safeguarding Policy
- Staff Code of Conduct
- Staff Handbook
- Storage and Retention of Records Policy
- Use of Images Policy

#### 4. Key data protection terms used in this Policy

- **Data controller** – an organisation 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 is the controller of pupils' personal information. As a data controller, we are responsible for safeguarding the use of personal data.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll 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 information (or 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). 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, 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.

#### 5. Data Protection Co-ordinator

The School has appointed its Compliance Officer as the Data Protection Co-ordinator (Privacy Officer), who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of applicable data protection legislation. 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 Privacy Officer.

#### 6. GDPR 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 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 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 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 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 GDPR (and the fact that it can be withdrawn by the data subject) it is generally considered preferable for the School 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 the Controller. It can be challenged by data subjects and also means 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 Policy, 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, 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 of all staff

### **a. Record-keeping**

- It is important that personal data held by the School is accurate, fair and adequate. Staff 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, pupils and their parents – in a way that is professional and appropriate.
- Staff 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 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 sometimes exist to withhold these from such requests. However, the starting position is to **record every document or email in a form they would be able to stand by should the person about whom it was recorded were to see it.**

### **b. Data handling**

- All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance with the Staff Handbook and all relevant School policies and procedures. In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and E-safety, so all staff should read and comply with the policies mentioned above.
- 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 obligations in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to 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 staff become aware of a personal data breach they must notify the 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 it may be minor, and it may involve fault or not, but the School always needs to know about them to make a decision.
- As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those affected, and could be a serious disciplinary matter whether under this Policy or the Staff member's contract.

#### **d. Care and data security**

- More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 6 above), and to 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 effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what their 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 information is used by the School to the Privacy Officer, and to identify the need for (and implement) regular staff training.

#### **e. Rights of Individuals**

- In addition to the School's 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. the School).
- This is known as the 'subject access right' (or the right to make 'subject access requests'). 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 Privacy Officer 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 (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 Privacy Officer as soon as possible.

#### **9. Data Security: online and digital**

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

As such:

- no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or Bursar;
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so;
- Where a member of staff is permitted to take data offsite it will need to be encrypted; and
- Use of personal email accounts or unencrypted personal devices for official School business is not permitted.

**Please also refer to the IT Acceptable, Remote Working: Access and Devices and Remote Learning policies.**

## **10. Processing of Financial / Credit Card Data**

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

## **11. Summary**

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

**Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how 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 need to be mindful of it. See Appendix 1 for the School's Data Protection Statement.**

### **Appendix 1:**



## **PARKSIDE SCHOOL Statement:**

### **Data Protection**

*Information provided by you will be used by the School.*

*It will be stored securely and used solely for the purpose that it was intended for in accordance with current data protection laws.*

*For more information about how the School will use your information, please see our Privacy Notice which is available on the School's website:*

*<http://www.parkside-school.co.uk>*

*or,*

*as a hard copy via request from the School Office.*

*May 2021*