ST PETER'S

PREPARATORY SCHOOL

Data Protection Policy

Updated on 2 April 2026
by Mr Dan Morris
(Director of Operations & Compliance)

Approved by Head: Charlotte P Johnston.

Date: 12th May 2026

Policy 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.

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

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? 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 was able to 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 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 need to be mindful of it.

1. Background

Data protection is an important legal compliance issue for St Peter's Preparatory 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, its contractors and other third parties (in a manner more fully detailed in the School's Privacy Notice. The School, as data "controller", is liable for the actions of its staff and Board of Reference 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 handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK 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 in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

2. Definitions

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

- **[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 Board of Reference) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.

- **[Data] Processor** – an organisation that processes personal data on behalf of a 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 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). 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.

- **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.

3. Application of this policy

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 Board of Reference] 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 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party controllers – which may range from other schools, to parents and appropriate authorities – 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.

If you are a volunteer [or contractor], you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

4. Person responsible for Data Protection at the School

The School has appointed the Director of Operations & Compliance as the Data Protection 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 Data Protection Officer.

5. The Principles

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

- Processed **lawfully, fairly** and in a **transparent** manner;
- Collected for **specific and explicit purposes** and only for the purposes it was collected for;

- **Relevant** and **limited** to what is necessary for the purposes it is processed;
- **Accurate** and kept **up to date**;
- **Kept for no longer than is necessary** for the purposes for which it is processed; and
- Processed in a manner that ensures **appropriate security** of the personal data.

The UK GDPR's broader '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 ("DPIA")); 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.

6. 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, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is 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 School. It can be challenged by data subjects and also means the School 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 the UK GDPR requires.

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 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.

7. Headline responsibilities for all staff

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 you 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 making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, 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 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**.

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 (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 should read and comply with the following policies:

- GDPR Privacy Notice, Taking, Storing and Using Images of Children Policy, Child Protection & Safeguarding Policy, CCTV Policy, Health and Safety Policy, IT Use Policy, Social Media Policy and e-Safety 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.

Avoiding, mitigating and reporting data breaches

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. Controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, 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 Director of Operations & Compliance. 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 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 applicable staff member's contract.

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 3 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 they 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 Director of Operations & Compliance, and to identity the need for (and implement) regular staff training. Staff must attend any training we require them to.

Use of third party platforms / suppliers

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the Director of Operations & Compliance in the first instance, and at as early a stage as possible.

8. 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 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 Director of Operations & Compliance 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; and
- 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 Director of Operations & Compliance 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.

- 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.
- 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.
- Use of personal email accounts by staff for official School business is not permitted.

Appendix A - Retention of Records / Archiving Documents

The GDPR requires that personal data is only retained for as long as necessary – that is, necessary for the specific lawful purpose (or purposes) it was acquired.

Therefore at the end of each school year the School evaluates its storage of personal and special category data and, in line with its Privacy notice, will retain, archive or destroy data accordingly.

The following table indicates the current DfE guidance on record retention to which the School adheres:

Type of Record/Document	Suggested Retention Period
SCHOOL-SPECIFIC RECORDS Registration documents of School Attendance Register Minutes of Board of Reference meetings Annual curriculum	 Permanent (or until closure of the school) 6 years from last date of entry, then archive. 6 years from date of meeting From end of year: 3 years (or 1 year for other class records: eg marks / timetables / assignments)
INDIVIDUAL PUPIL RECORDS Admissions: application forms, assessments, records of decisions Examination results (external or internal) Pupil file including: ● Pupil reports ● Pupil performance records ● Pupil medical records ● Special educational needs records (to be risk assessed individually)	**NB - this will generally be personal data** 25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision). 7 years from pupil leaving school ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil). Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)

SAFEGUARDING	NB – please read notice at the top of this note Keep a permanent record of historic policies
Policies and procedures	No longer than 6 months from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.
DBS disclosure certificates (if held)	Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available. [2]
Accident / Incident reporting	If a referral has been made / social care has been involved or child has been subject of a multi-agency plan – indefinitely.
Child Protection files	If low level concerns, with no multi-agency action – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).

Type of Record/Document	**Suggested[1] Retention Period**
CORPORATE RECORDS (where applicable)	e.g. where schools have trading arms
Certificates of Incorporation	Permanent (or until dissolution of the company)
Minutes, Notes and Resolutions of Boards or Management Meetings	Minimum – 10 years
Shareholder resolutions	Minimum – 10 years
Register of Members/Shareholders	Permanent (minimum 10 years for ex-members/shareholders)
Annual reports	Minimum – 6 years
ACCOUNTING RECORDS[3]	
Accounting records (normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state) [NB specific ambit to be advised by an accountancy expert]	Minimum – 3 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements
Tax returns	Minimum – 6 years

VAT returns	Minimum – 6 years
Budget and internal financial reports	Minimum – 3 years
CONTRACTS AND AGREEMENTS	
Signed or final/concluded agreements (plus any signed or final/concluded variations or amendments)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later
Deeds (or contracts under seal)	Minimum – 13 years from completion of contractual obligation or term of agreement
INTELLECTUAL PROPERTY RECORDS	
Formal documents of title (trade mark or registered design certificates; patent or utility model certificates)	Permanent (in the case of any right which can be permanently extended, e.g. trade marks); otherwise expiry of right plus minimum of 7 years.
Assignments of intellectual property to or from the School	As above in relation to contracts (7 years) or, where applicable, deeds (13 years).

Type of Record/Document	Suggested Retention Period
IP / IT agreements (including software licences and ancillary agreements e.g. maintenance; storage; development; coexistence agreements; consents)	Minimum – 7 years from completion of contractual obligation concerned or term of agreement
EMPLOYEE / PERSONNEL RECORDS Single Central Record of employees Contracts of employment Employee appraisals or reviews Staff personnel file Payroll, salary, maternity pay records Pension or other benefit schedule records Job application and interview/rejection records (unsuccessful applicants) Immigration records Health records relating to employees	NB this will contain personal data Keep a permanent record of all mandatory checks that have been undertaken (but not DBS certificate itself: 6 months as above) 7 years from effective date of end of contract Duration of employment plus minimum of 7 years As above, but do not delete any information which may be relevant to historic safeguarding claims. Minimum – 6 years Possibly permanent, depending on nature of scheme Minimum 3 months but no more than 1 year Minimum – 4 years 7 years from end of contract of employment
INSURANCE RECORDS Insurance policies (will vary – private, public, professional indemnity) Correspondence related to claims/ renewals/ notification re: insurance	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim. Minimum – 7 years
ENVIRONMENTAL, HEALTH & DATA Maintenance logs Accidents to children Accident at work records (staff) Staff use of hazardous substances	10 years from date of last entry 25 years from birth (longer for safeguarding) Minimum – 4 years from date of accident, but review case-by-case where possible

	Minimum – 7 years from end of date of use
Risk assessments (carried out in respect of above) [4] Data protection records documenting processing activity, data breaches	7 years from completion of relevant project, incident, event or activity No limit: as long as up-to-date and relevant (as long as no personal data held)
Emails on Server ● Pupil Email Accounts ● Staff Emails	● Delete upon leaving the school. ● Rescind Staff Access upon leaving employment, emails accessible by school admin for up to 3 years.

EXPLANATORY NOTES:

1. Some of these periods are mandatory legal requirements (e.g. under the Companies Act 2006 or the Charities Act 2011), but others are based on practical considerations for retention such as limitation periods for legal claims, and guidance from Courts, weighed against whether there is a reasonable argument in respect of data protection.

2. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches. It also found that it would be disproportionate for most organisations to conduct regular reviews, but at the time of writing the ICO (Information Commissioner's Office) still expects to see a responsible assessment policy (e.g. every 6 years) in place.

3. Retention period for tax purposes should <u>always</u> be made by reference to specific legal or accountancy advice.

4. As latent injuries can take years to manifest, the limitation period for claims reflects this: so records of procedures as they were at the time are also kept alongside relevant insurance documents.

Archive

Archived documentation is kept in the school secure archive store. Data is boxed, labelled and secured within the store.

Data to be destroyed

For confidential, sensitive or personal information to be considered securely disposed of, it must be in a condition where it cannot either be read or reconstructed. Therefore paper records are burned or shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, AV recordings and hard disks are dismantled and destroyed.

Where third party disposal experts are used, they are supervised wherever possible.

……

Acceptance

Please indicate with your name and signature below that you have read, understood and agree to comply with this data protection policy during and after your employment with SPL Education Ltd trading as "St Peter's Preparatory School"

Name (please print) ……

Position……

Signature …… Date ……..

Revision History		
Date Revised	**Changes**	**Reviewed By**
03 Apr 2025	Added Personal Breach Management and clarity around Legitimate Interests.	Dan Morris (Dir. of Operations)
02 Apr 2026	Adopted ISBA new model policy in its entirety.	Dan Morris (Dir. of Operations)