Data Protection Policy

1. Policy Statement

Sir William Perkins's School is a Charitable Company Limited by guarantee providing educational services for students of 11 to 18 years of age. Personal data is held and processed on parents/carers, children, employees and suppliers and others to provide these services.

The School has a clear objective to be compliant with General Data Protection Regulation and transparent in the use of personal data as is set out in the School data protection policy and privacy notices.

This policy applies to the storage and processing of personal data or sets of personal data in electronic form, including but not limited to databases, electronic mail, spreadsheet, word or other documents or where it is held in a paper format structured in a way that allows access to information about individuals.

This policy sets out how the School complies with the UK General Data Protection Regulation 2018 and how this is managed on an ongoing basis.

SWPS is fully committed to ensuring that the application of this Policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the School's Equal Opportunities Policy

2. Business Purposes

The School uses personal data, within the business, for providing education and pastoral care, personnel, administrative, financial, regulatory, payroll and business development purposes, including marketing.

Article 4 of the UK GDPR defines the following key terms:

a. **Personal data –** Any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data can be factual (for example, a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.
b. **Special Category data** – Personal data of or regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, generic data, biometric data, health, sex life or sexual orientation.
c. **Data Subject** – An identified, or identifiable natural person.
d. **Data Controller** – The natural or legal person, public authority, agency, or body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
e. **Processor** – A natural or legal person, public authority, agency or body which processes personal data on behalf of the controller.
f. **Third Party** – A body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
g. **Processing** – Any operation performed on personal data.

h. **Pseudonymisation** – Processing personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately.

i. **Personal data breach** – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, otherwise processed.

j. **Data Subject Consent** – Means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

k. **GDPR –** Has the meaning of UK GDPR and EU GDPR if applicable.

3. Procedures

3.1. The storage and processing of all personal data will be:

- Necessary for the School in the provision of education for the students;
- Stored for the minimal amount of time needed to achieve legitimate School needs;
- Secured with sufficient internal and external security to ensure only internal and third party personnel, who are authorised to access personal data, can access it;
- Removed at the request of the individual to whom the data refers through formal data subject access requests, if the right to erasure applies.

3.2. Justification for personal data

Personal data is processed in compliance with the six data privacy principles of good practice.

3.2.1. Personal data must be processed **lawfully, fairly,** and **in a transparent manner** in relation to the data subject.
3.2.2. Personal data can only be collected for specific, explicit, and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes.
3.2.3. Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. **(Data minimisation)**
3.2.4. Personal data must be **accurate** and kept up to date with every effort to erase or rectify without delay.
3.2.5. Personal data must be kept in a form such that the data subject can be identified only when necessary for processing. **(Storage limitation)**
3.2.6. Personal data must be processed in a manner that ensures the **appropriate security**, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical measures.

The controller must be able to demonstrate compliance with the GDPR's other principles by implementing policies, protection procedures, codes of conduct, response plans, etc. **(Accountability)**

3.3. Fair and lawful processing

Personal data is processed fairly and lawfully in accordance with individuals' rights.

The Schools privacy notices for students, and parents/carers, employees, contractors and volunteers, alumnae and special educational needs and disabilities, clearly define the

legal basis for collecting personal data either through consent, contract, legal obligation, vital interests, public task or legitimate interests depending upon the data set. A considerable portion of the School's personal data is processed on the basis it is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. When consent is required it is a clear active opt-in consent with a clearly stated process of how the data subject can opt-out at a later date.

The privacy notices contain:

- The information being collected;
- Why information is being collected;
- How and by whom it is collected
- How the information will be used;
- The legal basis for collecting the information;
- Where it is being stored;
- How long it shall be retained before deletion;
- Who it will be shared with;
- The existence of the right to request from the School access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- The existence of the right to withdraw consent;
- The existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- The right to lodge a complaint with the Commissioner;

3.4. Processing data in accordance with the individual's rights.

The School will ensure that personal data collected, stored or processed is accurate, adequate, relevant and not excessive. Personal data collected, stored or processed for one purpose will not be used for any unconnected purpose unless the individual concerned has agreed to it or would otherwise reasonably expect it through legitimate interests.

To ensure transparency and where there is a legitimate basis for opting out, the data subject can decline the use of their personal data. In this eventuality, the information is also deleted out of all storage including cache and back up storage.

All staff who are responsible for collecting, storing or processing personal data are aware of the conditions for collecting, storing and processing personal data as laid out in this policy.

Under GDPR entitlement data subjects have the following rights:

a. **Right to be informed –** the right to be told how their personal data is used in clear and transparent language.
b. **Right of access –** the right to know and have access to the personal data we have hold about them.
c. **Right to data portability –** the right to receive their data in a common and machine-readable electronic format.
d. **Right to be forgotten –** the right to have their personal data erased.
e. **Right to rectification –** the right to have their personal data corrected where it is inaccurate or incomplete.
f. **Right to object –** the right to complain and to object to processing.
g. **Right to purpose limitation** – the right to limit the extent of the processing of their personal data.
h. **Rights relates to automated decision-making and profiling –** the right not to be subject to decision without human involvement.

The School will comply with all valid requests, through a subject access request, unless an ICO exemption, such as legal requirement, applies.

3.5. Procedure for making requests:

Subject access requests from individuals should be made by email, addressed to the Director of Finance & Operations at dfo@swps.org.uk. The School will aim to provide the relevant data within one calendar month. Data will be provided in a commonly used, machine readable electronic format. (CSV, DOC or PDF).

3.6. Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the School will disclose requested data. However, the School will ensure the request is legitimate, seeking assistance from the board and from the School's legal advisers where necessary.

3.7. Consent

Where the data is subject to opt in consent by the data subject. The consent will be recorded and can be withdrawn at any time. Consent will be required for:

- Websites and tracking cookies;
- Marketing;
- Alumnae (due to individual financial analysis and analysis of individual's interests for event invitations);
- HR process for prospective employees;
- Child specific images;
- Trips for images and data;

Parents should be aware that, from around the age of 13, the law recognises students' own rights to have a say in how their personal information is used, as long as the child possesses the appropriate level of maturity. Parents should ensure that where consent is given on behalf of the child, that the child is made aware.

Where personal data processing is approved for marketing purposes, the data subject will be informed at the point of first contact that they have the right to object, at any stage, to having their data stored or processed for such purposes.

If the data subject puts forward an objection for marketing, the storage or processing of their personal data, for marketing, will cease immediately and their details will be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

3.8. Data retention

Personal data shall be retained for no longer than is necessary, however, necessary may be indefinitely for safeguarding and legal reasons.

The data retention of each data set is laid out in the data register. Once the retention period has expired it will be deleted off all systems internally and with any external providers.

3.9. Third Parties

The School will make sure all third parties engaged to store or process personal data on their behalf (i.e. data processors) are aware of and comply with the contents of this policy. Assurance of such compliance is obtained, whether companies or individuals, prior to granting them access to personal data controlled by the School.

3.10. Data security

Personal data, within the School, will be kept securely against loss, theft, damage, corruption or misuse. Where other organisations process personal data as a service, including IT services on behalf of the School, the Director of Finance & Operations will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

The School's IT Policies provide more information on IT security within the School.

3.11. International data transfers

No data is transferred outside of the EEA/UK without it being agreed by the Business Director who will ensure that the processing complies with the GDPR. Specific consent will be requested, where required, unless there is another legal or regulatory basis for this processing.

3.12. Criminal record checks

Where criminal record checks are required and justified by law they will be carried out. Criminal record checks are not undertaken based solely on the consent of the data subject.

3.13. Sensitive personal data or "Special Category Data"

In almost all cases explicit data subject's permission is required for storing, processing or passing on "Special Category Data" unless, under exceptional circumstances, there is a safe guarding or legal requirement that overrides this regulation. The Acceptance Form should only be signed once the School's Terms and Conditions and Privacy Notice have been noted.

Any exception to the data subject's rights will clearly state the relevant data that is being processed, the legal basis for processing it, to whom it is being disclosed and why.

3.14. Privacy by design and default

The School encompasses privacy by design and default as an approach to projects and applications. This approach promotes privacy and data protection compliance from the start through privacy impact assessments.

Where relevant, and when it does not have a negative impact on the data subject, privacy settings are set to the most private by default.

3.15. Data audit

Regular data audits, to manage and mitigate risks, will inform the data maps and registers. This contains information on what data is held, where it is stored, how it is used, who is responsible for it and any further regulations or retention timescales that may be relevant.

3.16. Reporting breaches

The School has a clear compliance failure and incident management process for detecting, containing and evaluating any personal data breach. Any breach will be reported to the Information Commissioners Office, ICO, as soon as possible but within the statutory 72 hours under the GDPR. Data subjects affected or potentially affected will be informed as soon as possible after the School becomes aware of any breach.

3.17. Internal employee personal data

Each employee, supplier, contractor or volunteer is responsible for taking steps to ensure that their personal data held is accurate and updated as required by the School.

3.18. Training

All employees and volunteers receive IT security and mandatory GDPR training through an online training portal. Contractors receive the relevant documents and training required to ensure GDPR compliance.

Refresher training is provided at least annually or whenever there is a substantial change in the law, this policy or associated procedure.

4. Consequences of failing to comply with this Data Protection Policy

The School takes compliance with this policy very seriously. Failure to comply puts students, parents/carers, employees, contractors, volunteers, other individuals and the organisation at risk and may lead to disciplinary action under the School's existing HR procedures, which may result in dismissal.

In the case of a contract or contractor it may lead to a breach of contract and thus termination of that contract.

5. Monitoring and Review

The Governing Body is ultimately responsible for the effective oversight, review and amendment of this policy and understands its legal obligation to do so.

This document will be reviewed and updated annually by the Director of Finance & Operations or as events or legislation requires.

Next scheduled review date: June 2026 *Last reviewed: June 2025*	
Key updates in this version:	• Updates to formatting/branding/job titles