



Privacy and Records Management

Important Note

Unless otherwise stated, all Policies of St Hilda's School apply to the school in its entirety. This comprises all staff and pupils in the Early Years Foundation Stage (EYFS), the Junior School (Key Stage 1) and the Senior School (Key Stage 2).

REVIEW DATE: APRIL 2019

REVIEWED BY: Dan Sayers (Headmaster)

SIGNED:

D. J. Sayers

DATED: 20.04.19

INTRODUCTION

As individuals we want to know that personal information about ourselves is handled properly. We and others have specific rights in this regard. In the course of its activities St Hilda's School collects, stores and processes personal data. The school recognises that the correct and lawful treatment of this data will maintain confidence in its organisation and is of importance to its successful operation.

The types of personal data that the school may be required to handle includes information about current, past and prospective employees, parents, pupils and others with whom it communicates. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the General Data Protection Regulations 2018 ("GDPR") and other regulations. GDPR imposes restrictions on how the school may process personal data. The school recognises that a breach of the GDPR could give rise to criminal sanctions as well as bad publicity.

WHO IS COVERED BY THE POLICY

This policy covers all those registered at the school as pupils, and all individuals employed by the school, irrespective of their status, level or grade. It therefore includes members of the Senior Management Team, Heads of Departments, teaching staff, non-teaching staff, part-time or fixed-term employees Peripatetic staff and volunteers (collectively referred to as employees in this policy).

STATUS OF THE POLICY

This policy has been approved by the school's Board of Governors. It sets out the school's rules on data protection and the eight data protection principles contained in it. These principles specify the legal conditions that must be satisfied in relation to the obtaining, handling, processing, transportation and storage of personal data.

The Headmaster is responsible for ensuring compliance with this policy. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Headmaster.

This policy is not part of the contract of employment of any employee and the school may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport and store personal data will adhere to the rules of the policy. Any breach of the policy will be taken seriously and may result in disciplinary action.

Any employee who considers that the policy has not been followed in respect of personal data about themselves or others should raise the matter with the school's Data Protection Compliance Manager in the first instance.

DEFINITION OF DATA PROTECTION TERMS

Data is recorded information whether stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom the School holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in possession of the school). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal or report card). It can even include a simple e-mail address. It is important that the information has the data subject as its focus or affects the individual's privacy in some way. Mere mention of someone's name in a document does not constitute personal data, but personal details such as someone's contact details or salary would still fall within the scope of the General Data Protection Regulations 2018.

Data controllers are the people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. The school is the data controller of all personal data used in its business.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the school's data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers that handle personal data on the school's behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

This policy is intended to provide information about how the school will use (or "process") personal data about individuals including: its staff; its current, past and prospective pupils; and their parents, carers or guardians (referred to in this policy as "parents").

DATA PROTECTION PRINCIPLES

Anyone processing personal data must comply with the eight enforceable principles of good practice.

These provide that personal data must be:

Processed fairly and lawfully:

- GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case the school), the purpose for which the data is to be processed by the school, and the identities of anyone to whom the data may be disclosed or transferred.
- For personal data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Processed for limited purposes and in an appropriate way:

- Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

Adequate, relevant and not excessive for the purpose:

- Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Accurate:

- Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Not kept longer than necessary for the purpose:

- Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from the School's systems when it is no longer required.

Processed in line with data subjects' rights:

Data must be processed in line with the data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller
- Prevent the processing of their data for direct-marketing purposes
- Ask to have inaccurate data amended
- Prevent processing that is likely to cause damage or distress to themselves or anyone else

Secure:

- 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. Data subjects may apply

to the courts for compensation if they have suffered damage from such a loss.

- GDPR requires the school to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

USE OF DATA

This policy applies alongside any other information the school may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This policy applies in addition to the school's other relevant terms and conditions and policies, including:

- any contract between the school and its staff or the parents of pupils;
- the school's policy on taking, storing and using images of children;
- the school's CCTV and/or biometrics policy;
- the school's retention of records policy;
- the school's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded; and
- the school's IT policies, including its Acceptable Use policy, eSafety policy, WiFi policy, Remote Working policy and Bring Your Own Device policy.

Anyone who works for, or acts on behalf of, the school (including staff, volunteers, governors and service providers) should also be aware of and comply with this Privacy Notice, which also provides further information about how personal data about those individuals will be used.

RESPONSIBILITY FOR DATA PROTECTION

The School has appointed the Compliance Officer, as Privacy and Compliance Officer who will deal with all your requests and enquiries concerning the school's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law. The Privacy and Compliance Officer can be contacted by email at administrator@sthildasharpندن.co.uk

WHY THE SCHOOL NEEDS TO PROCESS PERSONAL DATA

In order to carry out its ordinary duties to staff, pupils and parents, the school may process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the school will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the school's legitimate interests, or the legitimate interests of another, provided that these are not outweighed by the impact on individuals, and provided it does not involve special or sensitive types of data.

The school expects that the following uses may fall within that category of its (or its community's) "**legitimate interests**":

- For the purposes of pupil selection (and to confirm the identity of prospective pupils and their parents);
- To provide education services, including musical education, physical training or spiritual development, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
- Maintaining relationships with alumni and the school community, including direct marketing or fundraising activity;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- To enable relevant authorities to monitor the school's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the school;
- To safeguard pupils' welfare and provide appropriate pastoral care;
- To monitor (as appropriate) use of the school's IT and communications systems in accordance with the school's IT: acceptable use policy;
- To make use of photographic images of pupils in school publications, on the school website and (where appropriate) on the school's social media channels in accordance with the school's policy on taking, storing and using images of children;
- For security purposes, including CCTV in accordance with the school's CCTV policy; and
- Where otherwise reasonably necessary for the school's purposes, including to obtain appropriate professional advice and insurance for the school.

In addition, the school may need to process **special category personal data** (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or

duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so: for example for medical advice, social services, insurance purposes or to organisers of school trips;
- To provide educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- In connection with employment of its staff, for example DBS checks, welfare or pension plans; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example (but is not exhaustive):

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (about those who use our car parking facilities);
- bank details and other financial information, e.g. about parents who pay fees to the school;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the school about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the school's CCTV system (in accordance with the school's policy on taking, storing and using images of children);

HOW THE SCHOOL COLLECTS DATA

Generally, the school receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual); or collected from publicly available resources.

WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

Occasionally, the school will need to share personal information relating to its community with third parties, such as professional advisers (lawyers and accountants) or relevant authorities (HMRC, police or the local authority).

For the most part, personal data collected by the school will remain within the school, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of:

- medical records; and
- pastoral or safeguarding files.

However, a certain amount of any SEN pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

Staff, pupils and parents are reminded that the school is under duties imposed by law and statutory guidance (including [Keeping Children Safe in Education 2018](#)) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view the school's Safeguarding Policy.

Finally, in accordance with Data Protection Law, some of the school's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always subject to contractual assurances that personal data will be kept securely and only in accordance with the school's specific directions.

HOW LONG WE KEEP PERSONAL DATA

The school will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to 7 years following departure from the school. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the office. However, please bear in mind that the school may have lawful and necessary reasons to hold on to some data.

KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The school will use the contact details of parents, alumni and other members of the school community to keep them updated about the activities of the school, or

alumni and parent events of interest, including by sending updates and newsletters, by email and by post.

Should you wish to limit or object to any such use, or would like further information about them, please contact the office in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the school may need nonetheless to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

YOUR RIGHTS

Individuals have various rights under General Data Protection Regulations to access and understand personal data about them held by the school, and in some cases ask for it to be erased or amended or for the school to stop processing it, but subject to certain exemptions and limitations.

Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to the office.

The school will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is one month in the case of requests for access to information. The school will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the school may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The school is also not required to disclose any pupil examination scripts (though examiners' comments may fall to be disclosed), nor any confidential reference given by the school for the purposes of the education, training or employment of any individual.

PUPIL REQUESTS

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the school, they have sufficient maturity to understand the request they are making (see section Whose Rights below). Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's at law.

A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf. Moreover (if of sufficient age) their consent or authority may need to be sought by the parent making such a request. Pupils at Senior School / aged e.g. 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data

requested, including any relevant circumstances at home. Slightly younger children / Older Prep School children may however be sufficiently mature to have a say in this decision.

All information requests from, or on behalf of, pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

CONSENT

Where the school is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the school may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as an alumni or parents' association has been requested).

WHOSE RIGHTS

The rights under General Data Protection Regulations belong to the individual to whom the data relates. However, the school will often rely on parental consent to process personal data relating to pupils (if consent is required) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent.

Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances.

In general, the school will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the school's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the school may be under an obligation to maintain confidentiality unless, in the school's opinion, there is a good reason to do otherwise; for example where the school believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the school's IT: acceptable use policy and the school rules. Staff are under professional duties to do the same covered under the relevant staff policy.

DATA ACCURACY AND SECURITY

The school will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify the office of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under General Data Protection Regulations): please see above for details of why the school may need to process your data, of who you may contact if you disagree.

The school will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under General Data Protection Regulations and receive relevant training.

THIS POLICY

The school will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the Headmaster via email at administrator@sthildasharpenden.co.uk.

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with General Data Protection Regulations, they should utilise the school complaints procedure and should also notify the Headmaster. The school can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the school before involving the regulator.

This policy will be reviewed annually, by the Senior Management Team, in line with the school's review schedule for policies.