ST HELEN & ST KATHARINE

Michaelmas 2017

Data Protection Policy

For the purpose of this policy school personnel includes: volunteers, self-employed persons, employed staff and governors.

Introduction

This Data Protection Policy ("Policy") regulates and details the way in which St Helen and St Katharine ("the School") obtain, use, hold, transfer and process Personal Data and Sensitive Personal Data (as defined later in this policy) about individuals and ensures that all School personnel know the rules for protecting Personal Data.

This Policy also describes individuals' rights in relation to their Personal Data processed by the School.

The School has practices in place in relation to their handling of Personal Data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) due to be enacted in 2018.

The School shall comply with the principles of the DPA to ensure that all data is:

- Fairly and lawfully processed
- Processed only for lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to other countries without consent and adequate protection

In addition, the School will also comply with the GDPR that introduces further rights for individuals and strengthens some of the rights already in existence under the DPA, namely;

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

At all times, the School will endeavour to ensure that it has a legal basis for the processing of personal information.

St Helen and St Katharine is registered as a Data Controller with the Information Commissioner's Office (ICO). Our registration number is Z8494970. All data protection enquiries should be sent to data@shsk.org.uk

Personal Data

"Personal Data" is any information (for example, a person's name) or combination of information about a living person (such as name and address and date of birth) which allows that living person to be identified from that information and which relates to them, such as the job application of "Joe Green" with his address and date of birth, or the academic record of "Sophie Brown" with similar details. If in doubt, individual details should be treated as Personal Data.

Examples of Personal Data which may be used by the School in its day to day business include employee, student, parent and customer details, such as names, addresses, telephone numbers and other contact details, such as email addresses and mobile numbers, CVs, performance reviews, photos, payroll and salary information. This could affect job applicants, direct employees, temporary staff, volunteers, parents (including prospective parents), students, individual consultants or contractors, visitors etc.

Personal Data may also be relevant to unincorporated suppliers or customers or (such as a sole trader business or partnership), or inquirers or complainants, and to individual contacts at third parties, customers and leads, even in respect of work contact details, such as their direct line or mobile number, or information entered about them in any management system.

The laws governing how the School can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets).

Processing of Personal Data & Audits

The School uses or processes Personal Data (including Sensitive Personal Data, see relevant in this document) on a range of individuals for a multitude of business purposes, including the use of CCTV systems. Such individuals may include staff and contractors, students and parents (including prospective parents and students), alumnae, business contacts, customers and donors/investors, job applicants and former employees, and the person whose Personal Data is used by the School is known as "the data subject".

When the School collects, stores, uses, discloses, updates or deletes or destroys Personal Data, this is called "Processing". All processing is regulated by data protection legislation and must meet certain conditions to be carried out lawfully.

The School maintains a database of personal data held in different School departments, has clear retention schedules and the Compliance Administrator conducts regular audits of Personal Data held.

Personal Data and Sensitive Personal Data are held securely by the School and staff are periodically briefed on appropriate and safe data management.

Legislation and Information Commissioner's Office

Data protection laws are enforced in most countries by the local Data Protection Authority; in the UK this is the Information Commissioner's Office ("the "ICO"). The ICO may investigate concerns and complaints, may audit the School's use or processing of Personal Data and may take action against the School (and in some cases individuals) for breach of these laws. Action may include making the School pay a fine and/or stopping the use by the School of the Personal Data, which may prevent it from carrying on its business. Such action would cause reputational damage to the School and associated negative publicity.

The General Data Protection Regulation (GDPR) will replace the current EU Directive in 2018 and will be directly applicable in all Member States (and those wishing to engage and trade with those states) without the need for implementing national legislation. This introduces more stringent data protection obligations on Data Controllers.

Transparency and Personal Data

The School is entrusted to use the Personal Data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires the School to process Personal Data fairly.

In addition, use of Personal Data must be lawful. In practice, this means that the School will comply with at least one of the following conditions when processing Personal Data:

- the individual to whom the Personal Data relates has consented to the processing;
- the processing is necessary for the performance of a contract between the School and the individual (or to enter into that contract at the individual's request);
- the processing is necessary to comply with a legal obligation (not a contractual obligation) placed on the School;
- the processing is necessary to protect a vital interest of the individual (where there is an imminent risk to their life or of serious harm to them otherwise); or
- the processing is necessary to pursue the legitimate interest of the School (or a proposed recipient of the Personal Data) but where on balance, this would not involve disproportionate harm to the individual.

Use of Personal Data should meet one or more of these conditions. If there are any concerns about this; or it is proposed to use Personal Data for additional purposes; or new reasons for using Personal Data are envisaged, reliance on these conditions must be checked in advance by emailing the Compliance Administrator at: data@shsk.org.uk for advice.

All new Personal Data processing activities and projects involving the use of Personal Data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply. For example, if someone provides their details as a contact, you will not be able to start sending them marketing emails unless that is covered in an appropriate notice and consent from that individual.

In addition, the School ensures its Personal Data is accurate and up to date. The School takes care to record and input Personal Data accurately. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date and the School sends out annual data checking sheets to parents and staff and governors, so that inaccuracies can be amended. The School takes care to update records promptly and correctly.

Privacy Notices

When an individual gives the School any Personal Data about him or herself, the School will make sure the individual knows:

- who is responsible for the Processing of their Personal Data;
- for what purposes that School will process the Personal Data provided to it;
- sufficient details about any proposed disclosures/transfers of their Personal Data to Third Parties (including any cross border transfers);
- the rights that the individual has in respect of their personal data;
- any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations (retention periods for instance); and
- who to contact to discuss or raise any Personal Data issue.

The School does this by providing a "Data Protection Notice" or fair processing (privacy) notice. The Data Protection Notice is clearly displayed on the School Website. Before collecting Personal Data, staff at the School will give individuals providing those details specific Privacy Notices, these may be embedded in contracts, or on websites or form part of application or other forms, or simply signposting to the School's website. The School will inform individuals about the processing of their Personal Data before or at the time the data is collected. The information contained in its Privacy Notices will be concise and easily accessible and written in clear and plain language.

The School will only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s) already provided to an individual. Personal Data will not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

Sensitive Personal Data

"Sensitive Personal Data" is Personal Data about a person's race or ethnicity, their health, their sexual preference, their medical information, their religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. The Compliance Administrator can provide further information on what is Sensitive Personal Data and how it should be processed.

Sensitive Personal Data should not be collected or used unless essential. It must be treated as strictly confidential. **Extra care must be taken with it and it must be kept more securely**. In addition to the normal requirements for lawful use of any Personal Data, such details should not be used without the explicit prior consent of the individual, which has to be clear, unambiguous and voluntary.

The School does not seek to obtain Sensitive Personal Data unless:

- the individual concerned agrees in writing that we may do so, on the basis of a full understanding of why the School is collecting the data.
- the School needs to do so to meet its obligations or exercise its rights under any relevant laws; or
- in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned.

Please note that the “legitimate interest” criteria alone is not enough to process Sensitive Personal Data.

Sensitive Personal Data should not be disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the data is received by unintended recipients.

Sensitive Personal Data should be collected and used as little as possible and be subject to more limited and strictly need to know access and used subject to greater security measures than other Personal Data.

Other Personal Data where misuse may lead to distress or harm, especially to fraud or identity theft (for example, bank account or credit card details, or official government identification numbers, such as national insurance contribution numbers) must be treated like Sensitive Personal Data.

Employee Obligations

All School staff should be aware of their obligations and comply at all times with this Policy, updates to which will be communicated to all staff.

All staff must ensure that Personal Data collected by them must be appropriate to and sufficient for the relevant purpose(s) for which it is collected but not excessive for that purpose(s). Use of Personal Data should be minimised and not maximised. Collecting unnecessary personal Data adds to the School’s compliance burden. Where staff are dealing with student and parent data already collected by the School (on iSAMS for example), the individual/s concerned will have given consent on joining the School for the processing of their personal data for the purposes of running the School.

All staff involved in the processing of personal information will:

- Read and understand this policy
- Use strong passwords and two-step authentication
- Encrypt all portable devices if they contain personal data
- Only keep information as long as necessary

Staff should not download personal data onto personally owned devices unless absolutely necessary. In such cases, the personal data should be deleted from the personal device as soon as is practicable after use.

Data retention & School Archives

Personal Data must be stored securely and not be kept for any longer than required. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws).

As a general rule, when Personal Data is no longer needed for the purposes for which it was collected, this Personal Data will be securely and permanently destroyed as soon as practicable.

The School will not delete or destroy or amend records containing Personal Data without explicit consent once they have been informed those records have been requested by the

individual whose Personal Data it is, or by a Data Protection Authority. Such a breach may be a criminal offence with personal liability.

The School maintains a school archive of historical interest. This means that some data that is used for research purposes (and that is compatible with the purposes for which the data was originally collected) may be kept indefinitely if the relevant conditions apply. These are: that the data is not processed to support decisions about individuals, and that substantial damage or substantial distress is not likely to be caused to any data subject. Personal data can be selected for permanent preservation, and stored, if these two conditions apply, on condition that the other data protection principles are complied with.

The Right to Information, the Right to Erasure and Subject Access Requests

Individuals have certain rights in relation to their Personal Data:

- the right to obtain information (what Personal Data, from where, used for what purposes and shared with which recipients) about Personal Data held about themselves and to obtain copies of such Personal Data (Subject Access Request);
- the right to prevent processing of Personal Data for direct marketing purposes;
- the right to object to and stop certain processing of Personal Data where it is likely to cause substantial unwarranted harm or distress;
- the right to have Personal Data corrected;
- the right to compensation for any damage/distress suffered from any breach;
- the right to be informed of automated decision making about them.

If any member of School staff receives such a request or demand from an individual, they must promptly inform the Compliance Administrator.

Individuals are also allowed to withdraw their consent to the School's use of their Personal Data at any time. If a School employee receives such a withdrawal of consent, they must promptly inform the Compliance Administrator.

If anyone at the School receives a request to stop sending marketing materials, direct marketing communications of that type to that individual must be stopped as soon as is possible and the Compliance Administrator should be informed

Individuals can also ask in writing for copies of their Personal Data which the School holds about them and other details about how the School uses their Personal Data.

Subject to receipt of proof of ID where considered necessary (and payment of any official fee permitted which the School has requested), following receipt of a written request from an individual for access to his/her Personal Data, the School will (to the extent requested by the individual):

- Inform that individual whether the School holds Personal Data about him or her.
- Describe the Personal Data about the individual which it holds, the reason for holding the Personal Data and the categories of persons to whom it may disclose the Personal Data.
- Provide the individual with copies of the Personal Data held about him or her, together with an indication of the source(s) of the Personal Data.

Strict rules must be followed as part of this process. Therefore, any such request received should be passed on to the Compliance Administrator. There are strict statutory deadlines for responding. School staff must not respond to any such request directly.

There is a right under the DPA known as “the right to be forgotten”. This gives an individual the right to have their data erased when there is no compelling reason for continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this test is not present.

Data Security

The School endeavours to keep all Personal Data secure by protecting data against being accessed by other companies or individuals (for example, via hacking), from being corrupted (data corruption) or being lost or stolen. This applies to Personal Data in IT systems, emails and attachments and paper files.

School staff [and School Contractors and volunteers where relevant] each have a password and limited access rights to IT systems based on their role.

School staff must comply with the School’s security procedures whenever processing Personal Data. The School is dependent upon all employees to help keep Personal Data secure. Employees must only access and use Personal Data they are individually authorised to access and use and which is needed for a specific task within their School role.

School employees who work away from the School’s premises must comply with all requirements of the School’s Data Protection policy.

The School also recognises that adequate security is important where it arranges for Third Parties to process Personal Data and Sensitive Data on its behalf, such as when using service providers, who process Personal Data on behalf of the School. The School remains liable for those service providers and their treatment of the Personal Data. The School will have suitable written contracts in place with such service providers with specific terms included to protect the Personal Data provided to them.

Disclosing Personal Data to Third Parties and Overseas Transfers

A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. The School will not disclose Personal Data to a Third Party without first checking the disclosure is lawful and proportionate.

There are some exceptions to deal with disclosures, such as those requested lawfully by police where the information is necessary to prevent or detect a crime. Any request for Personal Data about an individual from government, police or other similar bodies or from journalists or other investigators should be passed immediately to the Compliance Administrator or in the case of safeguarding to the DSL.

From time to time the School may pass student personal data (including sensitive personal data where appropriate) to third parties where lawful to do so, including local authorities, other public authorities, independent school bodies such as the Independent Schools Inspectorate and the Independent Schools Council, health professionals and the School's professional advisers, and the examination boards, who will process the data:

- to enable the relevant authorities to monitor the School's performance;

- to compile statistical information (normally used on an anonymous basis);
- to secure funding for the School (and where relevant, on behalf of individual students);
- to safeguard students' welfare and provide appropriate pastoral (and where relevant, medical) care for students;
- where specifically requested by students and supported by their parents or guardians under legal and contractual obligations to provide this information;
- where necessary in connection with learning and extra-curricular activities undertaken by students;
- to enable students to take part in national and other assessments and to monitor students' progress and educational needs;
- to obtain appropriate professional advice and insurance for the School;
- where a reference or other information about a student or ex-student is requested by another educational establishment or employer to whom they have applied;
- where reasonably necessary for the operation of the School.

Unlawful disclosure (however well-meaning and however seemingly authoritative the requestor) risks placing the School in breach of several obligations under data protection legislation. Special care is needed with telephone requests for information, often used by unauthorised parties to obtain Personal Data to which they are not entitled. School employees must be certain of the identity of the person with whom they are dealing, they are to have a written request for information from them and ensure any disclosures are justified and authorised in advance.

There are special rules on whether Personal Data can be transferred to another country. Within the EU, there are restrictions on the transfer of Personal Data outside of the European Economic Area (EEA) (such a transfer can happen, for example, where Personal Data is emailed outside the EEA; where the School IT servers are hosted outside the EEA; or where there is remote on screen access from outside the EEA to Personal Data stored in an IT system within the EEA). This is to make sure the Personal Data remains safeguarded and that the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

Actual or likely transfers of Personal Data to outside the EEA, especially of Sensitive Personal Data, should be clearly set out in the privacy notices described in the fair use section of this Policy so that such transfers are expected by the affected individuals.

Alumnae, Marketing and Fundraising

As with other types of Processing, the use of Personal Data for marketing and fundraising purposes must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing has to be satisfied. Typically, this will have to be consent based.

Personal Data should not be used to contact individuals for marketing purposes by email, text or similar unless the individual has consented to marketing use. Individuals have a right to decline postal marketing and to object to any fundraising. Where marketing or fundraising is to be by phone, email, text or similar electronic means, normally individual consent is needed and must clearly cover marketing by that communication method. Special rules apply as to when consent is needed and how consent is obtained (for example, whether individuals can “opt out” of or “opt in” to receiving marketing) depending on the type of marketing contemplated and the means of communication with the individual. Any

objections to marketing or requests to unsubscribe must be dealt with properly and promptly.

School employees should liaise with the Compliance Administrator about any marketing or fundraising plans regarding compliance with regulation on Data Protection.

Policy last reviewed ……... Michaelmas 2017

Next Review date ……..…… Michaelmas 2018

Person Responsible …….. Bursar

Audience ……. Staff and Parents

Appendix 1

Key Summary and Guidance for SHSK School Staff - Data Protection

Background
80% of data breaches involve staff within an organisation (figure from the Information Commissioner's Office) and breaches, for the most part, are unintentional. Therefore everyone dealing with Personal Data needs to have a basic understanding of the Data Protection Act 1998 (DPA) and the new General Data Protection Directive (coming into force in 2018) that introduces more stringent data obligations.

The School collects a variety of personal data on students, parents, alumnae, contractors, staff, volunteers, business contacts etc for legitimate business reasons in connection with the running of the School. It is vital that all this information is kept securely, is regularly reviewed and disposed of when no longer required.

Data Protection Guidance
1. Read and follow the School's Data Protection Policy
2. Make sure all staff within your department are aware of the School's policy and departmental procedures on data protection
3. Use strong passwords on all devices and two step-authentication where possible. Ensure that any device you access school personal data on (mobiles for instance) are encrypted, password protected with remote wipe enabled.
4. External hard drives and memory sticks are not to be used to store personal data
5. Do not download personal data onto personally owned devices unless absolutely necessary. In such cases, any personal data should be permanently deleted from the personal device as soon as is possible after use.
6. Images must not be stored on any School or personally owned mobile device (refer to the Taking, Storing and Using Images of Students Policy)
6. Only keep information as long as necessary - conduct periodic reviews (at least yearly) of personal systems (paper and electronic) and delete personal data that is no longer required.
7. If in any doubt about any personal data issue, contact the School's Compliance Administrator (data@shsk.org.uk).

Guidance on keeping information secure
● Keep passwords secure – change these regularly and do not share or give other people your password. Use two step authentication.
● Always lock / log off computers when away from your desk
● Dispose of confidential paper waste securely by placing it in the shredding bags and then locking your office when unoccupied.
● Prevent virus attacks by taking care when opening emails and attachments or visiting new websites
● Hard copy personal information should be stored securely when it is not being used. In the case of hard copy Trip Packs containing sensitive data, these are to be stored in a lockable bag and secured on the person or in the boot of a locked car
● Be careful when discussing individuals that you are not in earshot of anyone who does not need access to that information
● Position computer screens away from windows and walkways to prevent accidental disclosures of personal or sensitive data
● Encrypt personal information that is being taken or sent outside the school or office.
● Do not, unless absolutely necessary, download personal data to a non-school device.

Guidance on keeping only relevant information:
● Collect only the personal information required.

● Explain new or changed business purposes to parents, students, employees and others, and obtain consent or provide an opt-out or opt-in where appropriate.
● Update records promptly – for example, changes of address, phone numbers.
● Delete personal information the School no longer requires. If in doubt, please check whether the information should be retained. In the case of safeguarding information, this should always be passed to the Designated Safeguarding Lead for her to decide whether or not the information should be retained.
● Be aware that there may be people who will try and trick staff into giving out personal information
● Carry out identity checks before giving out personal information to anyone in person, by writing or over the phone.

Handling requests from individuals for their personal information (subject access requests)
● People have a right to have a copy of the personal information the School holds
● Requests for Personal Data should be forwarded to the School's Compliance Administrator (data@shsk.org.uk).