ST HELEN & ST KATHARINE

Michaelmas 2018

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 Special Category 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 2018 (DPA) and the EU General Data Protection Regulation (GDPR) 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 Special Category Data, see relevant section 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 Co-ordinator conducts regular audits of Personal Data held.

Personal Data and Special Category 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 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 Coordinator 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.

Special Category Data

"Special Category 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 or trade union membership. The Compliance Co-ordinator can provide further information on what is Special Category Data and how it should be processed.

Special Category 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 Special Category 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 Special Category Data.

Special Category 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.

Special Category 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 Special Category 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 Co-ordinator.

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 Co-ordinator.

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 Co-ordinator 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, 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 Co-ordinator. 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 Co-ordinator or in the case of safeguarding to the DSL.

From time to time the School may pass student personal data (including Special Category 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 Special Category 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.

Data transfers outside of the EEA will be permissible where the recipient organisation is approved under the Privacy Shield mechanism.

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 Co-ordinator about any marketing or fundraising plans regarding compliance with regulation on Data Protection.

Appendix:

Information Security Procedure for SHSK School Personnel

Policy last reviewed …… Michaelmas 2018

Next Review date ……..…… Michaelmas 2019

Person Responsible …….. Bursar

Audience …….. Staff and Parents

Annex 1 – Information Security Procedure for SHSK School Personnel

Scope
Information security is about what you and the School should be doing to make sure that Personal Data is kept safe. This is the most important area of data protection to get right. Most data protection fines arise due to information security breaches.

This Annex should be read in conjunction with the School's Data Protection Policy, the School's privacy notices for staff, students and parents, and IT Acceptable Use Policy for staff.
Any questions or concerns about your obligations under this appendix should be referred to the Compliance Administrator (data@shsk.org.uk). Questions and concerns about technical support or for assistance with using the School IT systems should be referred to IT support (support@shsk.org.uk).

Awareness
You should immediately report all security incidents, breaches and weaknesses to the Bursar, or in his absence the Compliance Administrator (noting the separate procedure for out of school hours breaches in the trips guidance where the duty member of the SMT is contacted). This includes anything which you become aware of even if you are not directly involved. Examples of a security breach include but are not limited to:

- you accidently send an email to the wrong recipient or share email addresses through the cc box as opposed to bcc;
- you leave a hard copy of student medical information on a coach;
- any device (such as a laptop or a smartphone) you have used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

In certain situations, the School must report an information security breach to the Information Commissioner's Office and let those whose information has been compromised know within strict timescales.

Minimise the amount of Personal Data held
Only keep information as long as necessary - conduct periodic reviews (at least annually) of personal systems (paper and electronic) and delete personal data that is no longer required.

Be aware of phishing
Prevent virus attacks by taking care when opening emails and attachments or visiting new websites.

School Hardware and Software
Lock computer screens: Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time. To lock your computer screen press the "Windows" key followed by the "L" key. The school's staff computers are configured to automatically lock if not used for **15** minutes. Exam laptops and student laptops do not have auto lock.

Position computer screens away from windows and walkways to prevent accidental disclosures of personal or special category data.

Familiarise yourself with the School's IT: Ensure you are familiar with any software or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

- if you use Office 365 to share lesson resources and mock exam papers with students then you need to be careful that you do not accidently upload anything more confidential;
- make sure that you know how to properly use any security features contained in school software. For example, if you use software to redact documents ensure that the settings are configured so that the recipient of the document cannot "undo" the redactions

Hardware and software not provided by the School.
Staff must not use, download or install any software, app, programme, or service onto a School device without permission from the IT support team.

Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any non-School device or hardware to the School IT systems without permission.

Private cloud storage: You must not use private cloud storage or file sharing accounts to store or share School documents containing personal data.

Portable media devices: external hard drives/media and memory sticks are not to be used to store personal data

Disposal of School IT equipment
School IT equipment (this includes laptops, printers, phones, and DVDs) must always be returned to the IT Department even if you think that it is broken and will no longer work.

Passwords
Use strong, unique passwords on all devices and two step-authentication where possible. A strong password is one which is long, and the best incorporate a combination of letters numbers and characters which is easy for you to remember but not obvious to others. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

Passwords must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

Ensure that any device you access school personal data on (mobiles for instance) are encrypted, password protected with remote wipe enabled
.
Emails (and faxes)
When sending emails or faxes you must take care to make sure that the recipients are correct.

Files attached to emails which contain Special Category Data should be encrypted. Passwords for these attachments should be communicated separately.

Private email address and other forms of private electronic communication must not be used for School related work involving Personal Data.

Paper files

Keep securely: staff must ensure that papers which contain Personal Data are kept in a secure location and that they are never left unattended on desks unless the room is secure. Any keys must be kept safe.

Disposal: paper records containing Personal Data should be disposed of by placing it in the shredding bags and then locking your office when unoccupied. Personal Data should never be placed in the general waste.

Printing: when printing documents, make sure that you collect everything from the printer straight away if it is not a secure release device. If there is a problem with a secure release device when in the process of releasing your printing you need to alert IT support.

Put papers away: you should always keep a tidy desk and put papers away when they are no longer needed.

Post: you also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, consider asking your IT team to put in on an encrypted memory stick or arrange for it to be sent by courier.

Working off site or homeworking

Take the minimum with you. When working away from the School you must only take the minimum amount of information with you.

Paper records. If you need to take hard copy (i.e. paper) records with you which contain Personal Data then you should make sure that they are kept secure. For example:

- documents should be kept somewhere secure if left unattended (e.g. overnight);
- if travelling by train you must keep the documents with you at all times and they should not be stored in luggage racks;
- if travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights;
- if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should usually take them with you and keep them on your person in a locked case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case in the vehicle out of plain sight.

Special Category Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for school trips.

Working on the move: You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

Be careful when discussing individuals that you are not in earshot of anyone who does not need access to that information

Public Wi-Fi: care should be exercised when using public WiFi: you should only attempt to connect to WiFi which you are clear is bona fide – i.e. the credentials are provided to you by a trusted source, such as the host of as INSET venue. If you are in any way unsure as to the security of the WiFi network then you should not use it and rely only on 3G/4G.

For information regarding information security on school trips please read the guidance on page 3 of Events, Trips and Visits, Part A and B – core guidance to be read by all.

Using personal devices for School work
Any device you use to access School personal data must be protected with a strong, unique password and two-step authentication where possible. Ensure it is also encrypted and had remote wipe enabled.

Ensure that school email is accessed separately through the Outlook Web App, or in the case of a mobile phone/tablet it is accessed through the Outlook App for that device.

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.

Images must not be stored on any School or personally owned mobile device (refer to the Taking, Storing and Using Images of Students Policy)

You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything school related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working. You must also make sure that your devices are not configured in a way that would allow someone else access to School related documents and information – if you are unsure about this then please speak to the Data Services Manager. If you stop using your device for School work you must submit the device to IT support for wiping. You must provide all necessary co-operation and assistance to them in relation to this process.