SMANNELL FIELD SCHOOL

**GENERAL DATA PROTECTION REGULATION (GDPR) AND DATA PROTECTION ACT 2018**

**Policy Statement**

Everyone has rights with regards to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about our pupils and their families, suppliers and third parties.

We recognise that the correct and lawful treatment of this data will maintain confidence in our school and will provide for successful business operations.

School employees are obliged to comply with this policy when processing personal data on our behalf.

**About this policy**

The types of personal data that the school may be required to handle includes information about current, past and prospective pupils and others that we communicate with. 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 (GDPR) and the data protection act 2018 (together referred to as the Data Protection Legislation).

This policy, along with the school’s General Privacy Notice and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources and in accordance with the Data Protection Legislation.

This policy has been approved by the Governors of the school. It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process and store personal data.

The Data Protection Officer is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer at adminoffice@sfs.hants.sch.uk.

The Data Protection Officer will be responsible for completing the annual notification to the ICO and advising them of any updates to the register within 28-days.

**Definition of data protection terms**

**Data subjects** for the purpose of this policy includes all living individuals about whom we hold 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 our possession). Personal data can be factual (for example, a name, a unique reference number, address or date of birth) or it can be an opinion about that person, their actions or behaviours.

**Data controllers** are the people or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with GDPR. The school is the data controller for all personal data it collects or uses in its day to day business and in providing services.

**Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it includes suppliers, providers and contractors which handle personal data on the school’s behalf.

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

**Special category data** (also known as sensitive personal data) includes information revealing racial or ethnic origin. The definition also includes the processing of health data or data concerning sexual orientation. Special category data can only be processed under strict conditions. Personal data relating to criminal convictions and offences is subject to additional requirements and should be handled in a similar way to special category data.

**Third party** relates to any individual or organisation other than the data subject, the data controller, the school’s or its agents.

**Responsibilities under the General Data Protection Regulations (GDPR)**

The school is a data controller under GDPR; it is also a processor of information from other organisations (schools).

The Data Protection Officer is responsible for ensuring compliance with GDPR and with this policy and may assign staff to support this process.

The Governors through the Senior Leadership Team are responsible for developing and encouraging good information handling practice within the school.

Compliance with data protection legislation is the responsibility of everybody who processes personal data.

The school, through its staff is, is responsible for ensuring that any personal data supplied is accurate and up-to-date.

**Data protection principles**

Anyone processing personal data must comply with the six principles relating to processing of personal data in the GDPR. These provide that personal data must be **processed lawfully, fairly and in a transparent manner** in relation to the data subject. For personal data to be processed lawfully it must be processed on the basis of one of the legal grounds set out in GDPR.

These include, among other things, processing as necessary;

* For the performance of a task carried out by the school in the interest and pursuance of its duty
* For the performance of a contact to which the data subject is party
* For compliance with a legal duty
* The data subject has given consent for the data to be processed for a specific purpose

When special category date is being processed, additional conditions must be met. When processing personal data as data controllers in the course of the school’s business we will ensure that those requirements are met.

Data must be for collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes.

The school will only process personal data for the specific purpose permitted by the legislation. The school will notify those purposes to the data subject when we first collect the personal data or as soon as possible thereafter.

The school will only use data that is **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed, this is referred to as ‘**data minimisation**’.

Personal data, which is not strictly necessary for the purpose for which it is obtained will not be collected. If personal data is given or obtained which is excessive for the purpose it will be immediately deleted or destroyed.

The school will ensure that data is **accurate and where necessary kept up to date**; every reasonable step will be taken to ensure that personal data that is inaccurate (having regard for the purpose of which it is processed) is erased or rectified without detail. This will ensure **accuracy**.

Personal data which is kept for a long time must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that it is accurate. It is the

responsibility of the individual to ensure that personal data held by the school is accurate and up-to-date. Individuals should notify the school of any changes to enable personal records to be updated accordingly. It is the responsibility of the school to ensure that any notification regarding change is noted and acted upon.

Data will be **kept in a form which permits identification of data subjects for no longer than is necessary** for the purpose for which the personal data is processed.

The school will not keep personal data longer than is necessary for the purpose or purposes for which it is collected. All reasonable steps to destroy or erase data from our systems will be taken when the data is no longer required. On occasion personal data may be stored for longer periods as the personal data will be processed solely for archiving purposes in the public interest in accordance with Article 89(1).

Data will be **processed in a manner that ensures appropriate security of the personal data** including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures to ensure **integrity and confidentiality.**

**Notifying data subjects**

The school will inform data subjects, through our Privacy Notice, about;

* The purpose or purposes for which we intend to process the personal data
* The legal basis for processing the data
* The types of third parties, if any, with which the school shares or to which the school will discuss that personal data
* The length of time that we will retain the data
* The means, if any, with which data subjects can limit our use and disclosure of their personal data

If we receive personal data about a data subject from other sources (e.g. schools) our school will provide the data subject with information within the required timescales. We will also inform data subjects whose personal data we process that we are the data controller with regard to that data and with the contact details of the school’s Data Protection Officer (DPO).

**Data Security**

The school will take appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss or damage to personal data.

The school will 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 will only be transferred to a data processor who has provided sufficient guarantees to implement appropriate technical and organisational measures that will comply with the Data Protection legislation and ensure that data subject’s rights are protected and that these requirements are governed by a contract or other legally binding agreement.

The school will maintain data security by protecting the confidentiality, integrity and availability of the personal data defined as follows;

* **Confidentiality means** that only people who are authorised to use the personal data should access it
* **Integrity means** that personal data should be accurate and suitable for the purpose for which it is processed
* **Availability means** that authorised users should be able to access the personal data if they need it for authorised purposes

The **school’s security procedures** include;

* **Entry control**, the front door to the school remains locked at all times, entry can only be granted by an authorised person
* **Secure lockable cupboards and desks** are used and are kept locked if they contain confidential information
* **Paper documents that are no longer required are shredded** (on site)
* **Digital storage devices will be physically destroyed** when they are no longer required
* Individual monitors **do not show confidential information to passers-by** and staff log off from their PC if it is left unattended
* The school maintains up-to-date firewalls, patching and other security measures (controlled by the local authority IT services)

**School staff are trained** and this training includes;

* Mandatory training for all staff on Data Protection, with refresher training
* Training for specialist Data Protection staff and those who handle Subject Access Requests
* Training provided before access is provided to data systems

The **school’s governance and assurance procedures** include;

* All governors receive training with regards GDPR
* The school is open to and invites regular and audit by the local authority (Hampshire County Council)

**Disclosure and sharing of personal information**

The school will only disclose or share a data subject’s personal data where it is legally permitted to do so in order to comply with any legal obligation or in order to enforce or apply any contract with the data subject. This includes exchanging information with other parties or organisations for the purpose of risk reduction or fraud protection.

**Individual rights under GDPR**

Individuals have a number of rights under GDPR including;

* Ask the school if it holds personal information about them
* Ask what it is used for
* Being given a copy of the information (subject to some exemptions)
* Being given details about the purposes for which the school uses the information and other organisations or persons to whom it is disclosed
* Ask for incorrect data to be corrected
* To be given a copy of the information with any unintelligible terms explained
* Ask that information about them is erased (right to be forgotten)
* Ask the school not to use personal information for direct marketing
* Ask the school not to make decisions which significantly affect the individual based solely on the automatic processing of data

These rights are not absolute, if the school is not able to respond to a request it will outline the legal reasons for its decision clearly.

**Dealing with subject access request**

The school will provide a mechanism by which data subjects can make a request to access information held about them. There are some limited circumstances in which personal data relating to the applicant may be withheld. Examples of this include repeat access requests , confidential references and third party information.

Data subjects must make a formal request for information the school holds about them. This must be made in writing. All such requests should be forwarded to the DPO.

Any individual who wishes to exercise this right should provide satisfactory proof of identity and sufficient information to enable the data to be located.

Subject to satisfaction of proof the data controller should respond within 30 calendar days and in accordance with any relevant exemptions specified in the legislation.

**Retention and disposal of data**

The school discourages the retention of personal data for longer than it is required. Personal data must be disposed of in a way that protects the rights of privacy of data subjects.

Until further notice (and the completion of legal process) the school will maintain some information that is specific and relevant to other legal processes.

**Use of CCTV**

The school’s use of CCTV is regulated by the Surveillance Camera Commissioner and the school complies with the ICO Code of Practice.

**Data Breaches**

It is a requirements that data breaches are reported to the ICO within 72 hours where there is a privacy risk. Further there is a requirement to notify individuals affected where there is a high risk to their privacy.

Any suspected breaches at the school should be reported to the DPO immediately. The necessary reporting form is available from the DPO.

All staff are aware of their personal responsibility in this matter and, further, have completed training to reinforce this understanding.

The school’s DPO is Sarah Eaton.

**Freedom of Information Act 2000**

The Freedom of Information Act 2000 (FOIA) allows public access to all types of information held by public authorities. Requests for personal information will be dealt with under the Data Protection Act.