SUTTON VALENCE SCHOOL
SINCE 1576

Data Protection Policy

(Prep School and Senior School)

Author: Mr Glen Millbery
Policy Date: September 2025
Approval Date by Governors: November 2025
Review Date: September 2026

This Policy applies to Sutton Valence School (including as the context requires, the Nursery, the Prep School and Senior School).

Introduction

The information and guidelines within this policy are important and apply to all employees of the School.

Like all educational establishments, the School holds and processes information about its staff, pupils, ex-pupils and employees and other individuals for various purposes (for example, the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll and to enable correspondence and communications including the provision of references and certificates). To comply with data protection law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. This policy, so far as it is relevant, applies to personal information kept in manual or computerised files, whether or not those files comprise a relevant filing system, and therefore fall within the ambit of the GDPR.

Notification to the Data Protection Commissioner

The School has an obligation to notify the Information Commissioner of the purposes for which it processes personal data. Individual data subjects can obtain full details of the School's data protection register entry with the Information Commissioner from the School's Data Compliance Officer, or from the Information Commissioner's website (http://www.informationcommissioner.gov.uk/).

Data Compliance Officer

The School's Data Compliance Officer is Glen Millbery. All queries about the School policy and all requests for access to personal data should be addressed to the Data Compliance Officer.

Data Protection Principles

Sutton Valence School has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

> **Principle 1: Lawfulness, Fairness and Transparency.** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means we must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means we must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means we must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and kept up to date. This means we must have in place processes for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means we must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity and Confidentiality. Personal data shall 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. We must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

Principle 7: Accountability. The Data Controller shall be responsible for, and be able to demonstrate compliance. This means we must demonstrate that the six data protection principles (outlined above) are met for all personal data for which it is responsible.

Data Security and Disclosure

All members of School are responsible for ensuring that:

- any personal data which they hold is kept securely;
- personal data is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Personal data must be:

- kept in a locked filing cabinet, drawer or room;
- or if it is computerised, be password protected or kept only on a storage medium which is itself kept securely.

All appropriate security measures should be taken in addition to the two points above.

In addition to the requirements of the GDPR, the confidentiality of information about individuals must be respected.

Processing

Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission;
- dissemination or otherwise making available, or

- alignment, combination, blocking, erasure or destruction of the information or data.

External Privacy Notices

Each external website provided by Sutton Valence School will include an online Privacy Notice and an online Cookie Notice fulfilling the requirements of applicable law.

Responsibilities of Individual Data Users

All members of the School who record and/or process personal data in any form (called "Data Users" in this policy), must ensure that they comply with the requirements of the GDPR, and with the School's Data Protection Policy (including any procedures and guidelines which may be issued from time to time).

In particular, no member of the School or of the School staff may, without the prior authorisation of the Data Compliance Officer, in connection with his or her work in the School:

- develop a new computer system for processing personal data;
- use an existing computer system to process personal data for a purpose other than that already authorised;
- create a new manual filing system containing personal data;
- use an existing manual filing system containing personal data for a purpose other than that already authorised.

The above does not apply to databases which are maintained by individual data users within the School for their private domestic uses, i.e. private address books. However, individual data users should consider if their private uses fall within the scope of the GDPR.

Data Areas

Material falls within the ambit of the GDPR only if it is part of a structured filing system.

Computer Databases

Certain of the files referred to above are maintained in electronic databases as well as or instead of paper files. Access to such databases is restricted in the same manner as access to paper files.

In addition, however, the Network Manager and staff may have day-to-day access to the electronic databases for the purposes of administering and maintaining the same.

Employees and Pupils

Employees and pupils/contacts of pupils (parents/guardians) must ensure that any personal data provided to the School is accurate and up to date. They must ensure that any changes of address or other personal details are notified to the School.

Employees who use the School's computer facilities must not hold or process personal data about others except as authorised. In the case of sensitive personal data, if the data subject has not given their explicit consent or some other authority does not exist under the GDPR it is a crime.

Data Subjects' Consent

(a) Employees

The School will only hold and process personal data as is necessary for its proper purposes and does not need, therefore, except for sensitive personal data to seek the consent of

individual data subjects. In addition, all staff now consent explicitly to the processing by the School of personal data (including sensitive personal data) about them for employment purposes.

(b) Pupils, Parents and Guardians

The same processing criteria apply to pupils, parents and Guardians as set out in (a) above.

Right to Access Personal Data

Employees, pupils and other individuals have the right under the GDPR to access any personal data that is being held about them either in an "automatically processable form" (mainly computer records) or in "relevant filing systems" (i.e. highly structured files which enable personal data relating to a particular individual to be readily accessible) or to request the correction of such data where incorrect.

Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Compliance Officer who will take appropriate steps to make the necessary amendments.

Subject Access Request

There are two types of subject access request – one for the educational record and one for all information held. A request may include both elements.

The request can be made by the parent or by the child. If made by the parent, for a child 12 or over, the consent of the child must also be obtained.

The information includes:

- information held on computer (or other automated means);
- information held in structured files;
- information in the educational record regardless of the form in which it is held;
- unstructured information, for example, held in loose correspondence.

We must also include a description of the information, the purposes it is used for, who it is released to, and any information available about the source of the information. The information must be supplied in an intelligible form (so any codes should be explained) and should be in hard copy unless it is not possible to do this or would involve a disproportionate effort, or if the pupil or parent agrees to access the information in another form.

The Data Compliance Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access;
- Objection to processing;
- Objection to automated decision-making and profiling;
- Restriction of processing;
- Data portability;
- Data rectification;
- Data erasure.

If an individual makes a request relating to any of the rights listed above, we will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Detailed guidance for dealing with requests from data subjects can be found in the Subject Access Rights Policy and Procedure document.

Identification of Individual

The identity of the individual making the request and the consent of the child need to be verified.

Withholding Information

There are two situations when information may be withheld. The first is when the information is covered by an exemption in the Act. The second is when the request is unfounded or excessive.

The main exemptions when information may be withheld relate to:

- information which might cause serious harm to the physical or mental health of the pupil or another individual;
- cases where the disclosure would reveal a child is at risk of abuse;
- information contained in adoption and parental order records;
- information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992;
- copies of examination scripts;
- providing examination marks before they are officially announced.

If we possess the information and it does not fall into any of the categories above, there is no legal basis for the withholding of the information.

If information is withheld, a reason for the withholding of information will be given and attached to the information.

Educational Record

This will be the:

a. unique pupil number;
b. surname and where known, former surname;
c. forename(s);
d. date of birth;
e. gender;
f. ethnic group; and
g. first language;
h. Where the pupil has special educational needs, the type of special educational
i. provision that is being made for him ("School Action", "School Action Plus" or "Statement").

The following information in relation to the School year:

j. the total number of sessions in the School year;
k. the total number of sessions in that School year attended by the pupil;
l. the total number of the pupil's unauthorised absences in that School year;
m. the departmental number and name of the new school.

The pupil's cumulative achievements in education, as follows:

n. the results of the teacher assessment of the pupil's National Curriculum (NC) levels of attainment at the end of any key stage completed, excluding any such assessment in English at the end of the first key stage;
o. the results of the teacher assessment of his NC attainment targets;

p. where the pupil has not completed any key stage or is between key stages when he transfers school, the most recent assessment by the teacher of his NC levels of attainment, where any such assessments have been made;
q. the results of the NC tasks and NC tests taken by the pupil at the end of any key stage completed, by level and score;
r. the age-standardised scores, derived from tables produced by the Qualifications and Curriculum Authority, where these have been applied;
s. the NC test tiers, where appropriate;
t. the results of any public examinations taken, by subject and grade;
u. details of any vocational qualifications or credits towards any such qualifications gained;
v. copies of reports for the pupil.

All other Information

- information held on computer (or other automated means);
- information held in structured files;
- unstructured information, for example, held in loose correspondence.

For Sutton Valence School this will include:

- Financial information relating to the individual for whom the information request has been made;
- Emails concerning the individual;
- Praise, detentions and cause for concern;
- Copies of correspondence;
- Information within a teacher's mark book.

When referring to emails, the definition of personal data has recently changed, due to the decision in a case (Durant versus Financial Services Authority), in which it was decided that for information from which an individual can be recognised to be personal data, an additional requirement is that the information has to be focused on the individual, biographical in some significant sense, and if disclosed, likely to have an adverse effect on the privacy of that individual.

Redacting Information

If information relates to a third party, this information should not be given. This does not mean we cannot give any of the information, we need to remove references. The recommended method is to photocopy/print the document and then remove the names of the third party with a thick black marker. The document should then be photocopied again and this photocopy is the one to be handed over. It should be checked to make sure that there are no third party names within the document.

Handing Over Information

All information should be provided in the media that the request was made. Copies of the material handed over is retained in the School records.

Disclosure Outside of the EEA

The School may, from time to time and for its proper purposes, desire to transfer personal data to countries or territories outside of the European Economic Area.

Personal data, even if it would otherwise constitute fair processing, must not be disclosed or transferred outside the EEA without an individual data subject's consent, if the School is not satisfied that the country or territory in question ensures an adequate level of protection for the rights and freedoms of data subjects.

Sutton Valence School may only transfer personal data where one of the transfer scenarios listed below applies:

- The data subject has given Consent to the proposed transfer;
- The transfer is necessary for the performance of a contract with the data subject;
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject;
- The transfer is legally required on important public interest grounds;
- The transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of the data subject.

Sensitive Personal Data

The School may from time to time process "sensitive personal data" relating to members, staff and candidates.

Sensitive personal data is information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

Currently, the School envisages that the need to process sensitive personal data might include the following: data relating to the ethnic origin of employees or pupils of the School may be processed for the purposes of equal opportunities monitoring and for any necessary dietary requirements. Medical records need to be processed by healthcare professionals for the provision of healthcare and general welfare, for any necessary dietary requirements and accommodation issues and to assist in meeting the needs of employees and pupils with disabilities.

In exceptional circumstances, the School may need to process information regarding criminal convictions or alleged offences in connection, for example, with any disciplinary proceedings or other legal obligations.

In other circumstances, where sensitive personal data is to be held or processed, the School will seek the explicit consent of the member or staff member in question unless one of the limited exemptions provided in the GDPR applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

Data Processed for Research Purposes

Personal data held by the School may be processed for research purposes, including statistical or historical purposes. Personal data must not be used in this way if to do so would, or would be likely to, cause substantial damage or substantial distress to the individual data subject(s).

Accordingly, it is the School's policy for prior written approval to be obtained from the School Data Compliance Officer for any research involving personal data held by the School. Personal data used for research purposes must not be published or disclosed in any way in which the individual data subject can be identified.

CCTV

The School operates a number of CCTV cameras in order to assist with security for employees and pupils and in respect of School property. Any queries regarding the operation of the CCTV system should be raised with the Data Compliance Officer. An individual who wishes to exercise his/her right of access to any personal data about them on the CCTV system should complete the School "Access to Personal Data" form which is available from the Data Compliance Officer. As much information as possible should be given on the form to enable the data to be located (including, if possible, details of the relevant camera, date and time).

Email

It is permissible and appropriate for the School to keep records of internal communications which are relevant to an individual's ongoing relationship with the School, whether as an employee, member of staff or pupil, including information concerning performance and conduct issues, provided such records comply with the GDPR.

It is recognised that email is used for such communications and that such emails should form part of the School's records. It goes beyond the scope of this policy document to address the appropriate use of email in the proper functioning of the School, and the limitations and legal implications with this mode of communication. However, all employees of the School and pupils need to be aware that:

- the GDPR applies to emails which contain personal data about individuals which are sent or received by employees and pupils (other than for their own private purposes as opposed to School purposes);
- subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual subject can provide sufficient information for the School to locate the personal data in the emails; and
- the legislation applies to all emails from and to employees and pupils which are sent and received for School purposes, whether or not the emails are sent through the School email system, or on an individual's own email account (although this is in breach of the ICT Policies).

Electronic communications are dealt with specifically in the Electronic Communications Policy.

Complaints handling

Data subjects with a complaint about the processing of their personal data should put forward the matter in writing to the Data Compliance Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Compliance Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Compliance Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Compliance Officer providing a description of what occurred. The Data Compliance Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Compliance Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved. Further information can be found in the Data Breach Notification Policy and Procedure.

Compliance Monitoring

To confirm that an adequate level of compliance is being achieved by Sutton Valence School in relation to this policy, the Data Compliance Officer will carry out an annual data protection compliance audit. Each audit will, as a minimum, assess:

Compliance with policy in relation to the protection of personal data, including:

- The assignment of responsibilities;
- Raising awareness;
- Training of employees.

The effectiveness of data protection related operational practices, including:

- Data subject rights;
- Personal data transfers;
- Personal data incident management;
- Personal data complaints handling;
- The level of understanding of data protection policies and privacy notices;
- The currency of data protection policies and privacy notices;
- The accuracy of personal data being stored;
- The conformity of data processor activities;
- The adequacy of procedures for redressing poor compliance and personal data breaches.

The Data Compliance Officer will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame.

An annual report will be present to the Governing Body of Sutton Valence School detailing the above information.

Training

All employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, we provide regular Data Protection training and procedural guidance for staff.