# Data Protection Policy

## 1. Aims

Samuel Rhodes School aims to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of the school workforce, pupil/student, parent, Governor, visitors, contractor, consultant, or any other individual is done so in accordance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018) and the Privacy & Electronic Communications (EC Directive) Regulations (PECR) 2011.

This policy applies to all personal data processed by the school, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

## 2. Legislation & Guidance

This policy meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR, UK GDPR and DPA 2018. It is also based on the information provided by the Article 29 Working Party. Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to video surveillance, and the DBS Code of Practice in relation to handling sensitive information. Furthermore, this policy complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

## 3. Definitions

| Term | Definition |
|---|---|
| Data controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. |

| | |
|---|---|
| Data processor | A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the Controller's instruction. |
| Data subject | The identified or identifiable individual whose personal data is held or processed. |
| Consent | Freely given, specific, informed and unambiguous indication of the data subject's wishes via a statement or by a clear affirmative action, signifying agreement to a specific processing of personal data relating to them. |
| Personal data | Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a<br>• name,<br>• an identification number,<br>• location data,<br>• an online identifier or<br>• to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| Special categories of personal data | Personal data which is more sensitive and so needs more protection, including Information about an individual's:<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation<br>• History of offences, convictions or cautions *<br>* Note: Whilst criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care which is needed with this data set. |
| Processing | Any operation or set of operations which is performed on personal data or on sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.<br>Processing can be automated or manual. |
| Data breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

## 4. The Data Controller

The School collects and determines the processing for personal data relating to parents/carers, pupils, the school workforce, governors/volunteers, visitors and others, in addition they process data on the behalf of others therefore is a data controller and a data processor.

The School is registered as a data controller with the ICO and will renew this registration as legally required, the registration number is Z7797723.

## 5. Roles & Responsibilities

This policy applies to **all individuals** employed by our school, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action.

### 5.1 Governing body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

### 5.2 Data protection officer

The School has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO), the responsible contact is

Claire Mehegan, Data Protection Services, Grow Education Partners
London Diocesan House, 36 Causton Street, London, SW1P 4AU
Email: claire.mehegan@london.anglican.org
Telephone: 020 7932 1175

They are responsible for overseeing the implementation of this policy, along with any future development of this or related policies/guidelines and reviewing our compliance with data protection law.

Upon request the DPO can provide an annual report of the school's compliance status directly to the governing board and will report to the board their advice and recommendations on school data protection issues.

The DPO is a named point of contact for all Data Subjects whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their SLA for Service.

5.3 Representative of the data controller

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All employees

Employees (regardless of role) are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address, telephone number, or bank details.
- Reporting a Data Breach, Data Right Request, or Freedom of Information Request.
- Contacting the Data Protection Lead or DPO:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice/notification, or transfer personal data outside the United Kingdom
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

## 6. The Data Protection Principles

Data Protection is based on seven principles that the school must comply with.

These are that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

The Accountability principle ties these all together by requiring an organisation to take responsibility for complying with the other six principles. Including having appropriate measures and records in place to be able to demonstrate compliance.

This policy sets out how the school aims to comply with these principles.

## 7. Processing Personal Data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 lawful bases (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate) has freely given clear **consent.**
- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden).

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in data protection law.

These are where:

- The individual (or their parent/carer, where appropriate) has **given explicit consent.**
- It is necessary for the purposes of carrying out the **obligations and exercising specific rights** of the controller or of the data subject in the field of **employment** of a Data Controller or of a Data Subject.
- It is necessary to protect the **vital interests** of the Data Subject.
- Processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a **foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.**
- Personal Data has **manifestly been made public** by the Data Subject.
- There is the **establishment, exercise or defense of a legal claim**.
- There are reasons of **public interest** in the area of **public health**.
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the **assessment of the working capacity of the employee**, the medical diagnosis, the provision of health or social care or treatment).
- There are **archiving** purposes in the **public interest**.

Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice.
These privacy notices can be found in a location accessible and relevant to the data subjects.

- Pupils and Parents/Carers: website
- School Workforce (includes Trainees, Contractors and Consultants): shared policies drive
- Governors & Volunteers: signing in station
- Job Applicants: application pack
- Visitors: signing in station

Additional Copies of the Privacy Notices are available on request by contacting the school office.

7.2 Limitation, minimisation and accuracy
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data via our privacy notices.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Employees must only process personal data where it is necessary to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When personal data is required for longer, employees must ensure it is destroyed. This will be done in accordance with the school data retention policy, which states how long particular documents should be kept, and how they should be destroyed.

Copies of the Data Retention Policy can be obtained by contacting the school office.

**8. Sharing Personal Data**
In order to efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.
- We need to liaise with other agencies – we may seek consent when appropriate before doing this where possible.
- Our suppliers or contractors need data to enable us to provide services to our employees

and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place.
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies when required to do so, these include but are not limited to:

- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.

**9. Artifical intelligence (AI)**

(AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. The School recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool the School will treat this as a data breach, and will follow the personal data breach procedure outlined in this policy.

**10. Transferring data internationally**

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

**11. Individuals data protection rights**

11.1 Access rights

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we can:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- Give you a copy of the information in an intelligible form.

11.2 Other rights regarding your data:

You may also

- Withdraw their consent to processing at any time, this only relates to tasks which the school relies on consent to process the data.
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing

- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Refer a complaint to the ICO
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, individuals are asked to preferably submit their request in written format to assist with comprehension.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the request

If you would like to exercise any of the rights or requests listed above, please contact the school office

- school@srs.islington.sch.uk
- Samuel Rhodes School
- 11 Highbury New Park, London, N5 2EG
- 020 7704 7490

If an individual receives a request, they must immediately forward it to the School Business Manager.

We reserve the right to verify the requester's identification by asking for Photo ID, if this proves insufficient then further ID may be required.

In most cases, we will respond to requests within 1 month, as required under data protection legislation. However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

If the request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee which would only take into account administrative costs.

A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.

When responding to requests, we will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual; or
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child

In the event we refuse a request, we will tell the individual why and tell them they have the right to refer a complaint to the ICO.

Article 22 of the UK GDPR has additional rules to protect individuals from decisions made solely for the purpose of automated decision-making and profiling. The school does not carry out any automated decision-making and/or profiling on individuals.

11.3 Children and data rights/requests

An individual's data belongs to them therefore a child's data belongs to that child, and not the child's parents or carers.

However, children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12 most data requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

**12. Parental requests to see Educational Record**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

Requests should be made in writing to the school office and should include;

- Name of individual making the request and child who the education record belongs to
- Requesters correspondence address
- Requesters contact number and email address.

**13. Close circuit television (CCTV)**

We use CCTV in various locations around the school sites and premises for the detection and prevention of crime. However, footage may be used for additional reasons specified more fully in the CCTV Policy. We adhere to the ICO's code of practice for the use of video surveillance and provide training to staff in its use.

We do not need to ask individuals' permission to use CCTV, but in most instances we make it clear where individuals are being recorded, with security cameras that are clearly visible and accompanied by prominent signs explaining that CCTV is in use, and where it is not clear, directions will be given on how further information can be sought.

The full CCTV policy can be obtained from the school office. Any enquiries about the CCTV system and policy should be directed to the school office.

**14. Photographs & Videos**

As part of our school activities, we may take photographs and record images of individuals within our school.

The use of school photographs includes but is not limited to:

- Within school on notice boards and in school magazines, brochures, newsletters and prospectuses.
- Outside of school by external agencies and partners such as the school photographer, local and national newspapers and local and national campaigns we are involved with
- Online on our website or social media pages

We will obtain consent from the responsible individuals to use pupil images. When doing so we will clearly explain how the photograph and/or video will be collected and used to both the parent/carer and pupil when obtaining consent.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

You can withdraw consent by contacting the school office.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos – please contact the school office.

**15. Data Protection by Design & Default**

We will put measures in place to show that we have integrated data protection into all of our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations.
- Completing data privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sought from the DPO.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Periodic audits will be undertaken to monitor and review our privacy measures and make sure we are compliant.
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold; maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

**16. Data Security & Storage of Records**

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Our organisational and technical measures include, but are not limited to;

- Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use. We endorse a clear desk policy.

- Papers containing confidential personal data will not be left out on display when not in use unless there is a compelling lawful basis to do so e.g. Public Task to display Allergy information in the Medical Room.
- Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
- Employees, Pupils or Governors/Volunteers who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see School's Online & E- safety policy and user agreements).
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

**17. Disposal of Records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be rectified or updated unless it is no longer of use and therefore will also be disposed of securely.

For example, we will shred paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction.

When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

**18. Personal Data Breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

All potential or confirmed Data Breach incidents should be reported to the School Business Manager where they will be assigned a unique refence number and recorded in the school's data breach log.

Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours.

Examples of a Data Protection Breach include but are not limited to:

- Personal data being let unattended in a meeting room/in the staffroom/in the PPA room.
- Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent.
- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

**19. Training**

All employees and governors are provided with data protection training as part of their induction process.

Periodic refresher will be provided to adhere to ICO best practice or to respond to changes in legislation, guidance or the school's processes. Records of attendance will be kept ensuring that all data handlers receive appropriate training.

**20. Monitoring Arrangements**

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work they carry out.

They will work with School Data Protection Lead (School Business Manager) and the Lead Governor for Data Protection to ensure that this policy remains contemporaneous and appropriate.

This policy will be reviewed yearly, and changes recommended when appropriate. The Governors will be asked to sign off the policy review and any necessary changes.

**21. Links with Other Policies**

This data protection policy is linked to other policies including:

- Freedom of information policy (including publication scheme)
- Online and E-Safety Policy
- ICT User agreements
- Data retention schedule
- Emergency, business, continuity, recovery and restoration plan
- Safeguarding and Child Protection Policy

- CCTV Policy

**APPENDIX 1 – Personal Data Breach Procedure**

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

**Breach Notification**

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the School Business Manager who will make a decision whether to refer the matter to the Data Protection Officer (DPO).

Irrespective of whether the DPO is notified or not the response to the breach will follow the same path and be broken down into four distinct sections: **Investigation, Recovery, Reporting, Remedial Action.**

Investigation, Recovery and Reporting must be undertaken within **72hrs** of breach realization. This is the period of time which Data Protection Act 2018 allows for referral to the ICO or Data subjects.

**Stage 1: Investigation:**

All suspected breaches will be entered onto the "Data Breach Log" and assigned a unique reference number. All subsequent information will then be recorded on this log.

In addition, where required a corresponding file should be opened named after the unique reference number. All articles relating to the investigation, recovery and reporting should be stored within this file.

The first stages of the investigation into the breach report is to determine whether a breach has occurred by deciding if personal data has been accidentally or unlawfully mishandled. This will be done by assessing whether the data has been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

If a breach has been confirmed, then the severity of it will be assessed by considering:

- Data subject affected (vulnerability)Number of Data subjects affected.
- Data type lost, personal identifying/ special category,
- Specific Data Sets lost
- Number of Data sets
- Format of Data, electronic/paper.

**Stage 2 Recovery:**

Next stage is to contain and minimize the impact of the breach, this will be assisted by relevant staff members or data processors where necessary.

This may include but not be limited to:

- Contacting parties who may have received the data.
- Email Recovery
- Backup file restoration
- Requesting deletion of data.

If the data has been sent to the wrong individual and it has been requested to be deleted, confirmation of deletion should be attained in a written format for posterity.

The success or failure of the recovery must be recorded and will inform the reporting stage.

**Stage 3: Remedial Action.**

Once the detail of the breach is known and as recovery process is being undertaken an assessment needs to be made on what potential future action could be considered to prevent a similar breach reoccurring.

This will involve reviewing the processes and procedures which may have failed resulting in the breach.

Potential remedial actions may include, but are not limited to:

- Anonymizing and minimizing data
- Encrypted drives
- Secure access servers
- Strong password setting
- Training and support for staff and governors
- Encrypted email

All potential remedial action is to be recorded on the Data Log.

**Stage 4 Reporting:**

The investigator must decide who should be informed about the breach, affected data subjects

and/or the ICO

- Depending on the result of the containment efforts, the investigator will review the potential consequences, assess their seriousness and likelihood then make a decision about who needs to be informed. This will be partly determined by assessing if the risk of damage caused by the breach exceeds that of the damage that may be caused to the relationship through being informed.

If the risk of personal damage exceeds that of relationship, the Data Subjects will be promptly informed, in writing, all individuals whose personal data has been breached. This notification will set out:

  - A description, in clear and plain language, of the nature of the personal data breach
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The decision on whether to contact individuals will be documented.

A decision also needs to be made if the breach has reached the threshold to be reported to the ICO. This must be judged on a case-by-case basis.

To decide, the investigator will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:

  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorized reversal of pseudonymization (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The decision will be documented either way, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored the breach register.

- Where the ICO must be notified, this will be done via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the DPO will set out all known details of the breach including recovery attempts and their success. Potentially remedial action will be included if known.

If all the breach details are not yet known, then as much as is known should be reported to the ICO within 72 hours. The report will explain that there is a delay, the reasons why, and when the further information is expected to be known. Then the remaining information will be submitted as soon as possible

At the conclusion of all stages of the Data Breach a mini report can be supplied to the Headteacher and Governors to brief them the outcome and propose ways it can be prevented from occurring again.

This is to allow Governors to hold the school accountable as per the Accountability Principle.

**APPENDIX 2 – Model Privacy Notices**

**Samuel Rhodes School Privacy Notice for Pupils Parents / Carers**

**How we use pupil and parent/carer information**

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use **pupil & parent/carer** personal data.

We, Samuel Rhodes School, is the 'Data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

In this privacy notices all references to 'you / your' include both the pupil and the pupil's parents, both individually and collectively, unless otherwise specified.

**1. The personal data we collect and hold**

Personal data that we may collect, use, store, and share (when appropriate) about pupils & parents/carers includes, but is not limited to:

- Personal Information (such as name, date of birth, unique pupil number, parent's/carer's national insurance number).
- Contact details and preferences (such as telephone number, email address, postal address, for you and your emergency contacts).
- Assessment information (such as data scores, tracking, and internal/external testing).

- Protected characteristics, (such as ethnic background, religion or belief).
- Special educational needs information (such as EHCP's, statements, applications for support, care or support plans).
- Exclusion information.
- Relevant medical information (such as NHS information, health checks, physical and mental health care, immunisation status and allergies and medical conditions, including physical and mental health).
- Attendance information (such as sessions attended, number of absences and absence reasons).
- Safeguarding information.
- Details of any support received, including care packages, plans and support providers.
- Photographs (such as for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- Closed-circuit television (CCTV) images captured in school.
- Data about your use of the school's information and communications systems.
- Payment and banking details where required.

We may also hold data about pupils and parents/carers that we have received from other organisations, including other schools, local authorities and the Department for Education ("DfE"). A full breakdown of the information we collect on pupils & parents/carers can be requested by contacting the school office, school@srs.islington.sch.uk

**2. Why we collect and use this information**

The purpose of collecting and processing this data includes but is not limited to:

- Contacting you in relation to your child or to inform you about School events and updates
- Supporting pupil learning
- Monitoring and reporting on pupil progress
- Providing appropriate pastoral care
- Protecting pupil welfare and safeguarding
- Assessing the quality of our services
- Administering admissions waiting lists
- Carrying out research
- Complying with the law regarding data sharing
- Adhering to the statutory duties placed upon us by the Department for Education.

**3. The lawful basis on which we use this information**

This section contains information about the legal basis that we are relying on when handling your

information. These are defined under data protection legislation and for personally identifiably information are:

- You have given consent for one or more specific purposes
- Processing is necessary to comply with the school's legal obligations
- Processing is necessary to protect your vital interests
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education)
- Processing is necessary for the school's legitimate interests or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent
- It is necessary to fulfil the school's obligations or your obligations
- It is necessary to protect your vital interests
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- Reasons of public interest in the area of public health.

An example of how we use the information you provide is:

The submission of the school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996.

Putting the school census on a statutory basis:

- means that schools do not need to obtain parental or pupil consent to the provision of information
- ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils
- helps to ensure that returns are completed by schools.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

**4. Collecting pupil information**

While the majority of information we collect about pupils & parents/carers is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

## 5. Storing pupil data

We keep your information for as long as we need to in order to educate and look after our pupils. The majority of this will be stored in the pupil file and this file will follow the pupil whenever they move schools and will be retained by the last school the pupil attends.

Where we are legally required or have a lawful basis to do so we will keep some information after your child has left the School. This will be retained in line with our Data Retention Schedule, a copy of which can be requested by contacting the school office, school@srs.islington.sch.uk

To protect your data, we have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed. Further information can be found in our Data Protection Policy or upon request.

## 6. Data Sharing

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions (where the pupil is not resident in Islington, with their respective local authority).
- The Department for Education- to meet our legal obligations to share certain information.
- The pupil's family and representatives- such as in the event of an emergency.
- Educators and examining bodies- such as ensuring we adhere to examining regulations to guarantee the validity of examinations.
- Ofsted- during the course of a school inspection.
- Suppliers and service providers – to enable them to provide the service we have contracted them for.
- Central and local government.
- Our auditors- to ensure compliance with our legal obligations.
- Health authorities (NHS) - to ensure the wellbeing of pupils.
- Security organisations to create a secure workplace for all staff.
- Health and social welfare organisations.
- Professional advisers and consultants - for us to develop our services and best provide our public service.
- Charities and voluntary organisations.
- Police forces, courts, tribunals, security services - to create a secure workplace for all at the school.
- Professional bodies.
- Schools that the pupils attend after leaving us.

## 7. Transferring data internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

## 8. Why we share information

In order to successfully perform our key functions, we need to share personal data with organisations

For example, we share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

## 9. Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example, via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

## 10. Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass basic pupil information (name, address and date of birth) to our local authority and /or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services

- careers advisers.

Any additional information is provided only with opt-in consent from the parent or carer.
This right is transferred to the child / pupil once they reach the age 16.

Pupils aged 16+
We will also share basic information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers.

For more information about services for young people, please visit our local authority website.
If a student is over 16, the child (or the parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service. Please see the contact us section below on how to opt-out of this arrangement. For more information about young peoples' services, please go to the Directgov Young People page at https://www.gov.uk/topic/schools-colleges-childrens-services/support-for-children-young-people

**11. The National Pupil Database (NPD)**

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to https://find-npd-data.education.gov.uk/
The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website:

https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

**12. Data Protection Rights**

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data

protection legislation. However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

**Your Other Rights regarding your Data**:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing).
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied.
- Prevent the use of your personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you).
- Request a cease to any processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Submit a complaint to the ICO.
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Parents/carers also have a legal right to access to their child's educational record.

If you would like to exercise any of the rights or requests listed above, please contact the school office:

- school@srs.islington.sch.uk
- 11 Highbury New Park, London, N5 2EG
- 020 7704 7490

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, although individuals are asked to preferably submit their request in written format to assist with comprehension.
We reserve the to verify the requesters identity by asking for Photo ID. If this proves insufficient, then further ID may be required.

**13. Data Protection Breaches**

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you please contact the School Business Manager at Samuel Rhodes School and advise us without undue delay.

**14. Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. To make a complaint, please contact our independent data protection officer:

Claire Mehegan, Data Protection Services, Grow Education Partners
London Diocesan House, 36 Causton Street, London, SW1P 4AU
Email: claire.mehegan@london.anglican.org
Telephone: 020 7932 1175

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

**15. Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Bernadette Napleton, School Business Manager at Samuel Rhodes School or our independent Data Protection Officer, Claire Mehegan at Grow Education Partners.

**Samuel Rhodes School Privacy Notice for School Workforce**

How we use the School Workforce's information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

Samuel Rhodes School (the School) is the 'Data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

**1. The personal data we hold.**

Personal data that we may collect, use, store, and share (when appropriate) about those we employ or otherwise engage to work at our school includes, but is not restricted to:

- Personal Information (such as name, date of birth, national insurance number, next of kin, dependents, marital status).
- Contact details (such as telephone number, email address, postal address, for you and your emergency contacts).
- Protected characteristics (such as trade union membership, nationality, language, ethnic origin, sexual orientation and religion or belief, where this has been provided).
- Relevant medical information (such as physical or mental health conditions, including for any disabilities for which the organisation needs to make any reasonable adjustments to fulfil its duty of care).
- Information about your renumeration (such as salary, annual leave, pension, bank details, payroll records, tax status and benefits information).
- Information from pre-employment background checks (such as criminal record, online search).
- Recruitment information, (such as copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Qualifications and employment records (such as work history, job titles, working hours, training records and professional memberships).
- Assessments of your performance (such as appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence).
- Outcomes of any disciplinary and/or grievance procedures, including any warnings issued to you and related correspondence.
- Details of periods of absence (such as holiday, sickness, family leave, sabbatical, including the reasons for the leave).
- Photographs (for internal safeguarding & security purposes, school newsletters, media, and promotional purposes).
- Closed-circuit television (CCTV) footage.
- Data about your use of the school's information and communications system.

We may also hold personal data about you from third parties, such as references supplied by former employers, information provided during the completion of our pre-employment checks, and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

A full breakdown of the information we collect on the School Workforce can be requested by contacting Bernadette Napleton, napleton.b@srs.islington.sch.uk

**2. Why we collect and use this information**

The purpose of collecting and processing includes but is not limited to:

- Running the school in an effective and efficient manner.
- Enabling you to be paid and other benefits to be provided.
- Facilitating safeguarding as part of our safeguarding obligations towards pupils.
- Fulfilling our legal obligations in recruiting individuals to the school workforce.
- Supporting effective performance management and appraisal.
- Supporting effective management of the school workforce, along with the implementation of school policies and procedures.
- Providing feedback to your training centre and awarding body.
- Informing our recruitment and retention policies.
- Allowing better financial modelling, administration and planning.
- Providing references where requested.
- Equalities monitoring and reporting.
- Responding to any school workforce issues.
- Improving the management of workforce data across the sector.
- Supporting the work of the School Teachers' Review Body.
- Assessing the quality of our services.
- Complying with the law regarding data sharing.

**3. The lawful basis for using this data**

These are defined under data protection legislation and for personally identifiably information are:

- To fulfil a contract with you.
- You have given consent for one or more specific purposes.
- Processing is necessary to comply with the school's legal obligations.
- Processing is necessary to protect your vital interests.
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

- Processing is necessary for the school's legitimate interests or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent.
- Employment, social security and social protection.
- It is necessary to fulfil the school's obligations or your obligations.
- It is necessary to protect your vital interests.
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions).
- Reasons of public interest in the area of public health.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent and explain how you can withdraw consent if you wish to do so.

**4. Collecting this information**

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

**5. How we store your data**

We collect, store and process data for each member of the school workforce. The information is contained in a virtual or physical file which is kept secure and only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our retention policy, a copy of which can be requested from the school office.

**6. Transferring Data Internationally**

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

**7. Who we share information with**

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals.
- The Department for Education- to meet our legal obligations to share certain information.
- Educators and examining bodies-such as ensuring we adhere to examining regulations to guarantee the validity of examinations.
- Training centres and awarding bodies-in order to provide information and feedback on your performance.
- Your families and representatives- such as in the event of an emergency.
- Financial organisations e.g. Pension Scheme, HMRC.
- Ofsted-during the course of a school inspection.
- Suppliers and service providers – to enable them to provide the service we have contracted them for such as HR, payroll, IT.
- Central and local government- such as workforce analysis.
- Our auditors - to ensure compliance with our legal obligations.
- Health authorities (NHS) and Occupational Health and employee support schemes to ensure the wellbeing of our staff body.
- Health and social welfare organisations.
- Professional advisers and consultants- for us to develop our services and best provide our public service.
- Trade Unions and Professional Associations - to enable them to provide the service their members require.
- Charities and voluntary organisations.

- Police forces, courts, tribunals, Security organisations- to create a secure workplace for all staff.
- Professional bodies.
- Employment & recruitment agencies and future employers - to support reference requests.

**8. Why we share your information**

In order to successfully perform our key functions, we need to share personal data with organisations

For example, we are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment. We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

**9. Data collection requirements:**

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance.

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use.

Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data.
- The purpose for which it is required.
- The level and sensitivity of data requested; and
- The arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.
For more information about the department's data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
To contact the department: https://www.gov.uk/contact-dfe

**10. Data Protection Rights**

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.
If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- NOT provide information where it compromises the privacy of others
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

**Your Other Rights regarding your Data**:

You may:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing).

- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied.
- Prevent the use of your personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you).
- Request a cease to any processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Refer a complaint to the ICO.
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

If you would like to exercise any of the rights or requests listed above, please contact Bernadette Napleton

- Email: napleton.b@srs.islington.sch.uk
- 11 Highbury New Park, London, N5 2EG
- Telephone: 020 7704 7490

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, but individuals are asked to preferably submit their request in written format to assist with comprehension.
We reserve the to verify the requester's identity by asking for Photo ID. If this proves insufficient, then further ID may be required.

**11. Data Protection Breaches**

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you please contact Bernadette Napleton, School Business Manager and advise us without undue delay.

**12. Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our independent data protection officer:

Claire Mehegan, Data Protection Services, Grow Education Partners
London Diocesan House, 36 Causton Street, London, SW1P 4AU
Email: claire.mehegan@london.anglican.org
Telephone: 020 7932 1175

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

**13. Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Bernadette Napleton, School Business Manager at Samuel Rhodes School or our independent Data Protection Officer, Claire Mehegan at Grow Education Partners.

**Samuel Rhodes School Privacy Notice for Governors and Volunteers**

Under data protection law, individuals have a right to be informed about how the school uses any personal data we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals working with the school in a voluntary capacity, including governors.

Samuel Rhodes School, (the School) is the 'data controller' for the purposes of data protection law.

We have appointed Grow Education Partners Ltd as our data protection officer (DPO) and the responsible contact is Claire Mehegan (see 'Contact us' below).

## 1. The Personal Data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not limited to:

- Personal Information (such as name, date of birth, next of kin, dependents, marital status).
- Contact details (such as telephone number, email address, postal address, for you and your emergency contacts).
- Protected characteristics (such as trade union membership, nationality, language, ethnic origin, sexual orientation, health and religion or belief, where this has been provided).
- Relevant medical information (such as physical or mental health conditions, including for any disabilities which the organisation needs to make any reasonable adjustments to fulfil its duty of care).
- Qualifications, and employment records (such as work history, job titles, references, training records and professional memberships).
- Outcomes of any disciplinary and/or grievance procedures, including any warning issues to you and related correspondence.
- Governor performance information (Such as meeting attendance, visits, roles, and leadership responsibilities).
- Information about business and pecuniary interests.
- Information from background checks (such as criminal record, online search).
- Closed-circuit television (CCTV) footage.
- Data about your use of the school's information and communications system.
- Photographs (for internal safeguarding & security purposes, school newsletters, media, and promotional purposes).
- Payment and banking details where required (e.g. for expense claims).

We may also hold personal data about you from third parties, such as information supplied by the appointing body and from the Disclosure & Barring Service, in order to comply with our legal obligations and statutory guidance.

A full breakdown of the information we collect on Governors & Volunteers can be requested by contacting Bernadette Napleton, napleton.b@srs.islington.sch.uk

## 2. Why we collect and use this information

The reasons we collect and process this data includes but is not limited to:

- Establish and maintain effective governance.
- Meet statutory obligations for publishing and sharing voluntary individuals' details.

- Facilitate safeguarding as part of our safeguarding obligations towards pupils.
- Fulfil our legal obligations in appointing voluntary individuals.
- Support development.
- Equalities monitoring and reporting.
- Ensure that appropriate access arrangements can be provided for volunteers who require them.
- To comply with the law regarding data sharing.
- Respond to any school workforce issues.
- Undertake statutory reporting the Department for Education.

**3. The lawful basis on which we use this information**

Are defined under data protection legislation and for personally identifiably information are:

- Processing is necessary to fulfil a contract with you.
- You have given consent for one or more specific purposes.
- Processing is necessary to comply with the school's legal obligations.
- Processing is necessary to protect your vital interests.
- Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).
- Processing is necessary for the school's legitimate interests or the legitimate interests of a third party.

When we process special category information, which is deemed to be more sensitive, the following lawful basis are used:

- You have given explicit consent.
- Employment, social security, and social protection.
- It is necessary to fulfil the school's obligations or your obligations.
- It is necessary to protect your vital interests.
- Processing is carried out by a foundation or not-for-profit organisation (includes religious, political, or philosophical organisations and trade unions).
- Reasons of public interest around public health.

Where we have obtained consent to use personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent and explain how consent can be withdrawn.

**4. Collecting this information**

While the majority of the information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

**5. Storing your data**

Personal data is stored in accordance with our data retention policy.

We retain personal information about all volunteers. This information is kept secure and is only used for purposes directly relevant to your work with the school.

When your relationship with the school has ended, we will retain and dispose of your personal information in accordance with our Data Retention Schedule. A copy of this can be obtained by contacting the school office.

**6. Who we share information with**

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- The Department for Education- to meet our legal obligations to share certain information.
- Our local authority – to meet our legal obligations to share certain information with it, such as details of governors.
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as governor support and IT services.
- Training centres and awarding bodies-in order to share information and feedback on your performance.
- Your families and representatives- such as in the event of an emergency.
- Our auditors to ensure compliance with our legal obligations.
- Trade Unions and Professional Associations - to enable them to provide the service their members require.
- Professional advisers and consultants - for us to develop our services and best provide our public service.
- Employment & recruitment agencies and future employers - to support reference requests.
- Police forces, courts, tribunals, security organisations – to create a secure workplace for all at the school.
- Charities and voluntary organisations.

**7. Transferring data internationally**

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK

**8. Why we share your information**

In order to successfully perform our key functions, we need to share personal data with organisations, for example we share personal data with the Department for Education (DfE) on a statutory basis. Under s.538 of the Education Act 1996, and the Academies Financial Handbook, the Secretary of State requires boards to provide certain details they hold about people involved in governance, as volunteered by individuals, and the information kept up to date.

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

**9. Data Protection Rights**

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.

- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation. However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

**Your Other Rights regarding your Data**

You may:

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing).
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied.
- Prevent the use of your personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you).
- Request a cease to any processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Submit a complaint to the ICO.
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

If you would like to exercise any of the rights or requests listed above, please contact Bernadette Napleton

- Email: napleton.b@srs.islington.sch.uk
- 11 Highbury New Park, London, N5 2EG
- Telephone: 020 7704 7490

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, although individuals are asked to preferably submit their request in written format to assist with comprehension.

We reserve the to verify the requesters' identity by asking for Photo ID. If this proves insufficient, then further ID may be required.

**10. Data Protection Breaches**

If you suspect that your or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction or damage, we ask that you please contact Bernadette Napleton, School Business Manager at Samuel Rhodes School and advise us without undue delay.

**11. Complaints**

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our independent data protection officer:

Claire Mehegan, Data Protection Services, Grow Education Partners
London Diocesan House, 36 Causton Street, London, SW1P 4AU
Email: claire.mehegan@london.anglican.org
Telephone: 020 7932 1175

Alternatively, you can refer a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

**12. Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Bernadette Napleton, School Business Manager, napleton.b@srs.islington.sch.uk or our independent Data Protection Officer Claire Mehegan at Grow Education Partners.

**Samuel Rhodes School Privacy Notice for Visitors**

How we use Visitor Information

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about Visitors.

Samuel Rhodes School is the 'Data Controller' for the purposes of data protection law.

As a public body as we have appointed Grow Education Partners Ltd as our Data Protection Officer (DPO). The responsible contact is Claire Mehegan (see contact us below)

**1. The personal data we hold**

We process data relating to those visiting our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not limited to:

- Name
- Company/Institution details
- Vehicle Registration details
- Closed-circuit television Images (CCTV) images
- Disclosure and Barring Service details
- Photo ID.

**2. Why we collect and use this information**

The purpose of collecting and processing this data is to help us run the school efficiently, including but not limited to:

- Fulfilling our legal obligations in relation to Keeping Children Safe in Education
- Informing our operational procedures
- Complying with the law regarding data sharing.

**3. Our lawful basis for using this data**

This section contains information about the legal basis that we are relying on when handling your information. These are defined under Data Protection legislation and for personally identifiable information are:

- Processing is necessary to comply with the legal obligations of the school.

- Processing is necessary for tasks in the public interest or exercise of authority vested in the school (the provision of education).

**4. Storing your data**

Your data will be stored in the electronic visitor system for 7 years.

**5. Who we share information with**

In order for us to legally, effectively and efficiently function we are required to share data with appropriate third parties, including but not limited to:

- Ofsted - during a school inspection.
- Security organisations - to create a secure environment for all.
- Our auditors, to ensure our compliance with our legal obligations.
- Public bodies, such as NHS England.
- Professional advisers and consultants - for us to develop our services and best provide our public service.
- Police forces, courts, tribunals and security services.

**6. Your rights**

*How to access personal information we hold about you*

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- Give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

In most cases, we will respond to subject access requests within 1 month, as required under data protection legislation However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

*Your other rights regarding your data*

- Withdraw your consent to processing at any time (This only relates to data for which the school relies on consent as a lawful basis for processing).
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied.
- Prevent the use of your personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect you).
- Request a cease to any processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

If you would like to exercise any of the rights or requests listed above, please contact Bernadette Napleton

- Email: napleton.b@srs.islington.sch.uk
- 11 Highbury New Park, London, N5 2EG
- Telephone: 020 7704 7490

The School will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, but individuals are asked to preferably submit their request in written format to assist with comprehension.

We reserve the to verify the requester's identity by asking for photo ID. If this proves insufficient then further ID may be required.

Data Protection Breaches

If you suspect that yours or someone else's data has been subject to unauthorised or unlawful processing, accidental loss, destruction, or damage, we ask that you please contact the DPO or Bernadette Napleton, School Business Manager.

## 7. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer

Claire Mehegan, Data Protection Services, Grow Education Partners
London Diocesan House, 36 Causton Street, London, SW1P 4AU
Email: claire.mehegan@london.anglican.org
Telephone: 020 7932 1175

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

## 8. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact either our School Data Protection Lead, Bernadette Napleton, School Business Manager, napleton.b@srs.islington.sch.uk or our independent Data Protection Officer Claire Mehegan at Grow Education Partners

Current version reviewed by: Bernadette Napleton Next review date: October 2027