Schools for Every Child

Data Protection Policy

We are an education Trust that is committed to running dynamic, ever-improving schools. We work to make sure that every child feels they belong in their school where they feel safe and inspired by learning. For us, learning is an adventure. It is a privilege and a responsibility for all who work with us to ensure that the journey through school is exciting, challenging, caring and enriching, and that every child experiences joy, wonder, calm and success.

Approval Level	Board
Author	COO
Approval Date	March 26
Trust/Template/School level	Trust
Review cycle	Annual

"The purpose of governance is to provide confident, strategic leadership and to create robust accountability, oversight and assurance for educational and financial performance". (DfE)

Approval History

Committee Approval	**Status**	**Next Review Date**
Board 9th March 26	Review in progress Submitted for Ratification Live Policy	Mar'27

Policy Updates:

Addition of section 3.5 Artificial Intelligence

Contents

[Part 1: Introduction and Key Definitions]

[Part 2: Organisational Arrangements]

[Part 3: Detailed Arrangements and Procedures]

- **Data Management**
- **Third Party Suppliers Acting as Data Processors**
- **Consent**
- **Associated Policies and documentation**

1.1 Introduction

Schools for Every Child and its constituent schools (The Trust) needs to gather and use certain information about individuals. These individuals can include pupils, parents, employees, suppliers, business contacts and other people the Trust has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Trust's data protection standards — and to comply with the law.

This data protection policy ensures that the Trust:

- Complies with data protection law and follows good practice;
- Protects the rights of pupils, staff, parents and other stakeholders;
- Is open about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach.

This data protection policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
4. Accurate and kept up to date
5. Kept in a form which permits identification of data subjects for no longer than is necessary
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage

1.2 Key Definitions

Data

The DPA describes how organisations must collect, handle and store personal information ('data').

Data is any information that the Trust collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;

- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data.

Data can be stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Data Subject

A 'Data Subject' is someone whose details the Trust keeps on file. The data subject has the following rights under data protection legislation:

- to be informed;
- to have access to data stored about them (or their children);
- to rectification if there is an error in the data stored;
- to erasure if there is no longer a need for the school to keep their data;
- to restrict processing (e.g. limit what their data is used for);
- to object to data being shared or collected.

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with third parties such as the Department for Education override these rights (this is documented later in the policy under 'Privacy Notices').

Data Controller

The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf.

The Trust is the 'Data Controller'.

Data Processor

A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff, third party company or another organisation such as the police or Local Authority (LA).

Part 2: Organisational Arrangements

2.1 Overall Responsibility

The Trust will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

The Trust Board will:

- Establish and maintain a positive data protection culture.
- Ensure the CEO prepares a Data Protection policy for approval and adoption by the Board and to review and monitor the effectiveness of the policy.
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties.
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices.
- Monitor and review data protection issues.
- Ensure that the Trust provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities.
- Review and act upon data protection compliance reports from the Data Protection Officer.

CEO with the support of the headteachers will:

- Promote a positive data protection culture.
- Prepare a Data Protection Policy for approval by the Trust Board, revise as necessary and review on a regular basis, at least every two years.
- Ensure that all staff cooperate with the policy.
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training.
- Provide staff with equipment and resources to enable them to protect the data that they are processing.
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training.
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities.

Local School Boards will:

- Promote a positive data protection culture.
- Familiarise themselves and comply with the Data Protection Policy.
- Monitor the work of the headteacher in ensuring that the school and its staff complies with the Data Protection Policy.
- Receive updates on developments and breaches and monitor responses and the support provided by the DPO.

The Data Protection Officer will:

- Inform and advise the Trust of their obligations under data protection legislation.
- Monitor compliance with the legislation and report to the CEO on a termly basis.
- Cooperate with the supervisory authority (e.g. Information Commissioner's Office) and act as the main contact point for any issues.
- Seek advice from other organisations or professionals, such as the Information Commissioner's Office as and when necessary.
- Keep up to date with new developments in data protection issues for schools and trusts.
- Act upon information and advice on data protection and circulate to staff and governors.
- Design a data protection induction for all staff and keep records of that induction.
- Coordinate a response to a Subject Access Request.
- Coordinate a response to a data breach.

Staff at the school will:

- Familiarise themselves and comply with the Data Protection Policy.
- Comply with the Trust data protection arrangements.
- Follow the data breach reporting process.
- Attend data protection training as organised by the school.

Part 3: Detailed Arrangements & Procedures

3.1 Data Management

Data Registration

As Data Controller, the trust is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Data Protection Officer

As a public body, the Trust is required to appoint a Data Protection Officer (DPO).

At Schools for Every Child the DPO role is fulfilled by:

- SBM Services

The role of the DPO is to:

- Inform and advise the school/academy and the employees about obligations to comply with all relevant data protection laws;
- Monitor compliance with the relevant data protection laws;
- Be the first point of contact for supervisory authorities;
- Coordinate training on data protection for all key stakeholders in the Trust.

Data Protection Awareness

In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the school/academy).

Data Mapping

The Trust has documented all of the data that it collects within a 'Data Map'. This data inventory records:

- the data held
- what the data is used for
- how it is collected
- the legal basis or via consent
- how the data is stored
- what the retention period is
- who can access the data
- who is accountable for the data

- how the data is shared
- how the data is destroyed

It is the responsibility of the SLT to ensure the 'Data Map' is kept up to date. The map should be a live document and updated regularly.

3.2 Third Party Suppliers Acting as Data Processors

As Data Controller, the Trust is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all subcontractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These type of agreements include:-

- IT contracts and processes.
- Physical data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

Only third-party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

The DPO may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the school to confirm compliance with the DPA principles and obligations to assist the school in the event of a data breach or subject access request, or enquiries from the ICO.

The school must have the right to conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the school's data, which shall also include cooperation and eventual secure destruction or return of data.

The Trust has a 'Third Party Request for Information' form which must be used for third-party suppliers acting as a Data Processor for the school.

3.3 Consent

As a Trust we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Privacy Notices

In order to comply with the fair processing requirements of the DPA, each school will inform their staff, parents and governors of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff, parents and governors through the following means:

- School and Trust websites
- Via the school offices
- Staff and governor internal drives and communications

The Use of Pupil Data - images and recordings

Occasionally the Trust may take photographs of its pupils. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

Each school will seek consent from all parents to allow images and recordings of pupils and the subsequent reproduction of these images. Consent will be sought on an annual basis.

Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in.

Generic consent for all uses of images is not acceptable; parents must give consent to each medium.

Parents must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school, however a verbal withdrawal of consent is also valid and should be reported to the headteacher immediately.

Consent should be recorded on the school MIS.

If images of individual pupils are published, then the name of that child should not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

The Trust 'Parental Consent' form should be issued to current parents to seek consent annually.

Accurate Data

The school will endeavour to ensure that the data it stores is accurate and up to date.

When a pupil or member of staff joins the Trust they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the Trust will also seek consent to use the information provided for other internal purposes (such as promoting school events, photography).

The school will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the Trust to use the information held for internal purposes.

Parents/carers and staff are requested to inform the Trust when their personal information changes.

Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school

will consider each situation on its merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to complete a Withdrawal of Consent form and return this to the school office of the relevant school.

3.4 Associated Data Protection Policies and Documentation

- CCTV - Appendix 1
- Complaints
- Data Breach Report
- Records Management
- Subject Access Requests Process
- Third Party Requests for Information Template
- Use of Personal Devices

CCTV

The Trust uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. The Trust has a CCTV Policy in place which documents:

- why CCTV is used
- where cameras are sited
- whether covert monitoring is undertaken
- how long images are retained for
- who has access to the images
- what the complaints procedure is

Complaints

Complaints will be dealt with in accordance with the Trust's Complaints Procedure. An individual may contact the Information Commissioner's Office (ICO) if they are not satisfied with how a complaint has been dealt with by the school. The telephone number for the ICO is 0303 123 1113.

Data Breaches

Although the Trust takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone).
- Inappropriate access controls allowing unauthorised use.
- Equipment failure.
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space).
- Unforeseen circumstances such as fire or flood.
- Hacking attack.
- 'Blagging' offences where information is obtained by deceiving the Trust.

The school has a Data Breach Policy which sets out the process that should be followed in the event of a data breach occurring.

Privacy Impact Assessments

When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the DPO. If risks are identified as part of the assessment then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'high risk' then the DPO should consult with the ICO prior to implementation.

The 'Data Privacy Impact Assessment' form must be used for each new service/product.

Records Management

The Trust recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

The Trust has a Record Management & Retention Policy in place which sets out how it will:

- safely and securely store data (both digital and hard copy data)
- retain data
- dispose of data

Subject Access Requests

Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/academy holds about them, and can make a Subject Access Request (SAR).

The Trust has a Subject Access Request Process, available on the Trust website.

Third Party Requests for Information

Occasionally the Trust may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The Trust has a Third Party Request for Information Process, available on the Trust website.

Use of Personal Devices

The Trust recognises the benefits of mobile technology and is committed to supporting staff in the acceptable use of mobile devices. This is outlined in the staff Code of Conduct - *IT and Acceptable Use*.

Biometric Data

Students and their parents are notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent before we take any biometric data from their child and first process it.

Students and their parents have the right to choose not to use the Trust's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.
Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object.

CCTV Policy

Biometric Data

Please refer to the Data Protection Policy for details regarding the biometric information held by the Trust. The Trust does not use any automated biometric recognition systems nor facial recognition software on its sites.

As per the Data Protection Policy, any changes to this will be communicated with parents prior to implementation.

3.5 Artificial intelligence (AI)

Artificial intelligence (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. Schools for Every Child 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, Schools for Every Child will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.