ST AIDAN'S
Voluntary Controlled
PRIMARY SCHOOL
Albany Road
London N4 4RR
T: 020 8340 2352
F: 020 8341 2320
E: admin@staidansprimaryschool.org.uk
W:www.staidansprimaryschool.org.uk

General data protection regulation policy

Introduction

At St Aidan's we aim 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, parent, Governor, visitor, 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 and Electronic Communications (EC Directive) Regulations (PECR) 2003.

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. This policy should be read together with other associated policies: *Freedom of information*, *E-safety*, *Asset management*, *Emergency action plan*, *Safeguarding and child protection* and the *Home-school agreement*.

Contents

1	**Legislation and guidance**	**2**
2	**Definitions**	**2**
3	**The data controller**	**3**
4	**Roles and responsibilities**	**3**
5	**The Data Protection principles**	**4**
6	**Processing personal data**	**4**
7	**Biometric recognition systems**	**5**
8	**Sharing personal data**	**5**
9	**Transferring Data Internationally**	**6**
10	**Artificial intelligence**	**6**
11	**Individuals' data rights**	**6**
12	**Parental requests to see the educational record**	**8**
13	**CCTV (closed-circuit television)**	**8**
14	**Photographs and videos**	**8**
15	**Data protection by design and default**	**9**
16	**Data security and storage of records**	**9**
17	**Disposal of records**	**10**
18	**Personal data breaches**	**10**
19	**Training**	**10**
20	**Monitoring and review**	**11**

1 Legislation and 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, PECR 2003, 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.

2 Definitions

Data controller
The 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 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 by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data
Any information relating to an identified or identifiable person ('data subject').

- an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a:
  - name;
  - an identification number;
  - location data;
  - an online identifier;
  - to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Special categories of personal data
Personal data which is more sensitive and so needs more protection, including information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetics;
- biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes;

- health – physical or mental;
- sex life or sexual orientation;
- history of offences, convictions or cautions.

Note: whilst criminal offences are not usually classified as 'special, we have included them in this policy in acknowledgement of the care 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.

- 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.

3 The data controller

At St Aidan's we collect and determine the processing for personal data relating to parents/carers, pupils, the school workforce, governors/volunteers, visitors and others, in addition, we process data on behalf of others and therefore are considered a data controller and a data processor.

3.1 St Aidan's is registered as a data controller with the ICO and will renew this registration as legally required, the registration number is Z6127039

4 Roles and responsibilities

This policy applies to all staff employed at the school and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

4.1 **Governing Body**
The Governing Body (GB) has overall responsibility for ensuring that the school complies with all relevant data protection obligations.

4.2 **Data Protection Officer**
The School has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO), the responsible contact is **David Coy** who is contactable at: david.coy@london.anglican.org

- 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 Body and will report to the GB 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.

- Note: Full details of the DPO's responsibilities are set out in the Service Level Agreement (SLA).

4.3 **Headteacher**

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

4.4 **Staff**

All staff (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, e.g. a change of address, telephone number, or bank details.
- Reporting a Data Breach, Data Rights 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, deal with data protection rights invoked by an individual, 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.

5 The Data Protection principles

Data Protection is based on seven data protection principles with which all organisations must comply. These are that 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 key principles.

6 Processing personal data

6.1 **Lawfulness, fairness and transparency**

- 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.**
- The Personal Data has **manifestly been made public** by the Data Subject;
- There is the **establishment, exercise or defence 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;

Whenever we first 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, available on our website or from the school office on request.

6.2 **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 in 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.
- We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
- When personal data is no longer required, 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* are available on our website or from the school office on request**.**

7 Biometric recognition systems

We do not use biometric recognition systems at St Aidan's and will inform parents/carers if we plan to do so in the future.

8 Sharing personal data

8.1 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 or services (we will seek consent as necessary before doing this where possible);
- our suppliers or contractors need data to enable us to provide services to our staff 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.

8.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so for:

- 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.

8.3 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 staff.

9 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;
- we communicate with you when you are overseas.

9.1 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 the EEA.

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

9.2 When organisations 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 adequate legal provisions are in place to transfer data outside the UK.

10 Artificial intelligence

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. We recognise 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. Any such action will be treated as a data breach, and the personal data breach procedure, outlined in this policy, will be followed

11 Individuals' data rights

Subject access requests

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.

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;
- 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;
- is contained in adoption or parental order records;
- is given to a court in proceedings concerning the child.

Other rights regarding your data

You may also:

- withdraw consent to processing at any time (this only relates to tasks which the school relies on consent to process;
- 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 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).

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

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

11.3 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.

11.4 If we refuse a request, we will tell you why and tell you of your right to refer a complaint to the ICO.

11.5 We will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, however, written requests are preferable to ensure clarity. They should include:

- name of individual;
- correspondence address;
- contact number and email address;
- details of the request.

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

11.7 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;
- 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;
- is contained in adoption or parental order records;
- is given to a court in proceedings concerning the child

11.8 **Children and subject access 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, so most requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a firm 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 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 the 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 submission of a written request. These should be made in writing to the DPO and should include:

- name of the individual;
- contact details – address, telephone numbers and email address.

13 CCTV (closed-circuit television)

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 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.

13.1 Details of CCTV can be found by contacting the school office.

14 Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their children for communication, marketing and promotional materials. We will clearly explain how the photographs and/or videos will be used to both the parent/carer and pupil.

14.1 We use photographs:

- within the school on notice boards and in school magazines, brochures, newsletters and prospectuses;
- outside 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.

Photographs and videos used in these ways will not be accompanied by any personal information about the child other than the first name.

14.2 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.

15 Data protection by design and 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 sort 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 and 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 and 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. In particular our or organisational and technical measures include:

- 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;

- papers containing confidential personal data will not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- passwords that are at least 8 characters long, containing letters and numbers are used to access school computers, laptops and other electronic devices. Those who use school-controlled devices or platforms are reminded to change their passwords at regular intervals
- encryption software is used to protect all portable devices and removable media, such as laptops, tablets and USB devices;
- staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our *E-safety policy* for further information);
- 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 also be disposed of securely, where we cannot or do not need to rectify or update it. 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 our 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. We keep a record of destruction log detailing records disposed of as part of the Data Retention schedule.

18 Personal data breaches

We 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 Headteacher, who will enter it into the data breach log using a unique reference number. 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.

- The full procedure is set out in the School's *Breach management polic*y, which is available on our website or from the school office on request.

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

- Personal data being left 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 staff and governors are provided with data protection training as part of their induction process. Periodic refresher training 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 and review

Working with the school's Data Protection Lead and Lead Governor for Data Protection, it is the responsibility of the DPO to monitor and review this policy as part of the general monitoring and compliance work undertaken.

20.1 This policy will be reviewed annually and amended as necessary. The revised document will be considered by the Care & Communication committee and ratified by the full Governing Body.

Date of policy: JULY 2024

Policy ratified: …….. (Signature) 8th July 2024 (Date)

Review due: JULY 2025