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
Headteacher: Anne Etchells

General data protection regulation policy

Introduction

At St Aidan's we aim to ensure that all personal data collected, stored, processed or destroyed about any person, whether a member of staff, pupil, parent, governor, visitor, contractor, consultant, a member of supply staff or other individual at the School is done in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the forthcoming revised Data Protection Act (2018) as set out in the current Data Protection Bill. This policy will be reviewed in line with the implementation of this new legislation. It applies to all personal data 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 in conjunction with other associated policies: Freedom of information, E-safety, Asset management, Emergency action plan, Safeguarding, Child protection and the Home-school agreement.

Contents

1 Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the Data Protection Act (2018). It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It is also based on the IC guidance on GDPR, and information provided by the Article 29 Working Party.

It meets the requirements of the Protection of Freedoms Act (2012), ICO's code of practice in relation to CCTV usage, and the DBS Code of Practice in relation to handling sensitive information. This policy also complies with the Education (Pupil Information) (England) Regulations (2005), which gives parents the right of access to their child's educational record.

2 Definitions

Term	Definition
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 or • 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 classified as “sensitive data” within GDPR, 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, whether or not by automated means, 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 process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore the school is a data controller and a data processor.

3.1 St Aidan's is registered as a data controller with the IC and will renew this registration annually or as otherwise legally required.

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 our school complies with all relevant data protection obligations.

4.2 **Data Protection Officer**

The Data Protection Officer (DPO) for the school is **Robert Bullett** and is contactable at: Robert.Bullett@london.anglican.org, or on: 020 7932 1161.

- The DPO is responsible for overseeing the implementation of this policy in the first instance, before reviewing our compliance with data protection law, and developing related policies and guidelines where applicable.
- The DPO will provide an annual report of school’s compliance and risk issues directly to the GB and will advise the GB on all school data protection issues.
- The DPO is the first point of contact for individuals 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.
- Contacting the 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 European Economic Area;
  - if there has been a data breach;
  - 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 GDPR principles

The GDPR is based on 6 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.

6 Collecting personal data

6.1 **Lawfulness, fairness and transparency**

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

a. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

b. 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.

c. The data needs to be processed so that the school can comply with a legal obligation

d. The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone’s life.

e. 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.

f. 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).

6.2 For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act (2018). These are where:

a. The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent.
b. It is necessary to fulfil the obligations of controller or of data subject.
c. It is necessary to protect the vital interests of the data subject.
d. Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions).
e. The personal data has manifestly been made public by the data subject.
f. There is the establishment, exercise or defence of a legal claim.
g. There are reasons of public interest in the area of public health.
h. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.
i. There are archiving purposes in the public interest.
j. The Government has varied the definition of a special category.

6.3 If we decide to offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent for this (except for online counselling and preventive services).

6.4 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, which can be found on the school website. Hard copies are available on request.

6.5 **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.
- Staff may only process personal data where it is necessary in order to do their jobs.
- When personal data is no longer required, staff must ensure it is deleted.

7 Sharing personal data

7.1 We will not normally share personal data with anyone else, but may do so 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.

7.2 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.

7.3 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.

7.4 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law, and will consult with affected individuals first.

8 Individuals' rights under GDPR

8.1 **Subject access requests**

Individuals have a right to make a 'subject access request' to access personal information that we hold about them. This includes:

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual;
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

8.2 Whilst we will comply with the GDPR in regard to dealing with all subject access requests submitted in any written format, we would prefer requests to be made by letter or email addressed to, or marked for the attention of, the DPO. They should include:

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

8.3 If staff receive a subject access request they must immediately forward it to the DPO.

8.4 **Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

- Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access 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.

8.5 **Responding to subject access requests**

When responding to requests, we may ask the individual to provide 2 forms of identification from the list below:

- passport;
- driving licence;
- utility bills with the current address;
- birth / marriage certificate;
- P45/P60;
- credit card or mortgage statement.

We may also contact the individual via phone to confirm the request was made and will:

- respond without delay and within 1 month (30 calendar days) of receipt of the request;
- provide the information free of charge;
  - we may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this as soon as possible, and explain why the extension is necessary.

8.6 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.

8.7 If the request is 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 unfounded or excessive if it is repetitive, or asks for further copies of the same information.
- When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

8.8 **Other data protection rights of the individual**

In addition to the right to make a subject access request and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- withdraw their consent to processing at any time;
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it in certain circumstances;
- prevent use of their personal data for direct marketing;
- challenge processing which has been justified on the basis of public interest;

- request a copy of agreements under which their personal data is transferred outside the European Economic Area;
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- prevent 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 their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

8.9 Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

9 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 receipt of a written request.

9.1 Requests should be made in writing to the DPO and should include:

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

10 CCTV

CCTV (closed circuit television) cameras are positioned in various locations around the site to ensure safety and security at the school. We adhere to the ICO's code of practice for the use of CCTV, and provide training to staff in its proper use.

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

Any enquiries about the CCTV system should be directed to the DPO.

11 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 child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or videos will be used to both the parent/carer and pupil.

11.1 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 this way will not be accompanied by any other personal information about the child, to ensure they cannot be identified.

11.2 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.

12 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.
- Regular (at least annual) training for members of staff on data protection law, this policy and any related policies and any other data protection matters. Records of attendance will be kept to record the training sessions, and ensure that all data handlers receive appropriate training.
- Termly reviews and audits to test 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.

13 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. Staff and pupils 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.

14 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 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. This is then recorded on our systems.

15 Personal data breaches

We will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in the CofE Primary School Breach Management Policy.

Where appropriate, we will report the data breach to the IC within 72 hours. Such breaches in a school context may include, but are not limited to:

- a non-anonymised data set 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.

16 Monitoring and review

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work they carry out. The Care and communication committee will be involved in the review process.

16.1 This policy will normally be under a two yearly review, but with the introduction of the Data Protection Act (2019) following Brexit, the review period has been shortened in the first instance.

Date of policy: MAY 2018

Policy ratified: …….. (Signature) …… (Date)

Review due: MAY 2019