Stanley St Andrew's Church of England Primary School

Data Protection Policy

As a church school we believe that every person, every child, and every adult is unique and special with God given gifts and talents which is our job to nurture and cherish.

Stanley St Andrew's Church of England Primary School is responsible for the day-to-day management of data that is held about pupils, staff, parents, carers and other individuals in connection with that school. We are committed to working effectively to provide a secure environment to protect data that we hold and store. Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for your data, and we take that very seriously. We have a number of policies and documents listed below which are related to data protection and these set out how we look after and use data and these are referenced throughout this policy. Each of these policies/documents is available on our school website and paper copies can be obtained by contacting the school office.

Commented [JW1]: Amend accordingly

Linked policies/documents:

- Privacy Notices (for Staff/Pupils/Governors/Job Applicants/School Trips/General)
- Retention of Records
- Confidentiality
- Information Sharing
- Breach & Non-Compliance Procedure
- Complaints Procedure
- Acceptable Use of IT, the Internet and Electronic Communication Policy
- Code of Conduct for Staff and Volunteers
- Confidentiality Policy
- ICT Policy
- CCTV Policy
- My Rights – A Guide for Data Subjects

What is the General Data Protection Regulation (UK GDPR)?

This is a European Directive that was brought into UK law with an updated Data Protection Act 2018 (DPA) in May 2018. It was brought into line with changes to the UK leaving the EU on 31 December 2020.

The UK GDPR and DPA 2018 exist to look after individuals' data. It is a series of safeguards

for every individual. Information about individuals needs to be treated with respect and be secure.

The UK GDPR exists to protect individual rights in an increasingly digital world.

Who does it apply to?

Everyone, including schools. As 'Public Bodies' schools and trusts have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the Data Protection Act 2018.

We want to make sure information about pupils, parents, staff and volunteers is kept secure and within the law.

What is Data?

Any information that relates to a living person that identifies them. This can be by name, address, or phone number for example. It also relates to details about that person, which can include opinions.

Some data is considered to be more sensitive, and therefore more important to protect. This is information about 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 where processed to uniquely identify a person.

Schools often collect sensitive data for DfE and LA requirements and of course pupil data may contain information about safeguarding, SEND or health needs. Information about other family members may also be on the school file.

Our privacy notices explain how data about specific groups or activities is used and stored.

What are the key principles of the UK GDPR?

Lawfulness, transparency and fairness

Schools must have a legitimate reason to hold the data, and we explain this in our privacy notices. We often ask for consent to use data about a pupil for a particular purpose. If you wish to withdraw consent, we have a form to complete to allow us to process your request. There are certain times when you cannot withdraw consent as explained in 'Data Subjects' Rights'.

Collect data for a specific purpose and use it for that purpose

Data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.

Limited collection

Data Controllers should only collect the minimum amount of data needed for a particular task or reason. This ensures that if there is a breach or a hack only limited information can be lost.

Accuracy

Data collected should be accurate, and steps should be taken to check and confirm accuracy. This is done when pupils join the school and is reviewed on an annual basis.

If a Data Subject feels that the information held is inaccurate, or should no longer be held by the Controller, or should not be held by the Controller in any event, a dispute resolution process and complaint process can be accessed. Initially an approach should be made directly to our school.

Retention

A retention of records policy is in place that governs how long records are held for.

Security

We have processes in place to keep data safe. That might be paper files, electronic records or other information. Please see the following policies for further information on data security:

- Acceptable Use of IT, the Internet and Electronic Communication Policy
- Code of Conduct for Staff and Volunteers
- Confidentiality Policy
- ICT Policy

Who is a 'data subject'?

A data subject is any individual whose details we keep on file. Some details are more sensitive than others. The UK GDPR sets out collection of details such as health conditions and ethnicity which are more sensitive than names and phone numbers.

Data subjects' rights

Individuals have a right:

- to be informed
- of access to data stored about them or their children
- to rectification if there is an error on the data stored
- to erasure if there is no longer a need for school to keep the data
- to restrict processing, i.e. to limit what is done with their data
- to object to data being shared or collected

There are also other rights that relate to automated decision making and data portability that are not directly relevant in schools.

Data subjects' rights are also subject to child protection and safeguarding concerns and sharing information for the prevention and detection of crime. Schools also have legal and contractual obligations to share information with organisations such as the Department for Education, Social Care, the Local Authority and HMRC amongst others. In some cases, these obligations override individual rights.

These Data Subject's Rights are set out in more detail in the document 'My Rights – A Guide

for Data Subjects'.

Subject Access Requests

You can ask for copies of information that we hold about you or a pupil (who you have parental responsibility for). This is known as a Subject Access Request (SAR). The process for SARs is set out on our website. If you wish to make a SAR, you should fill out the subject access request form. We may ask you to provide identification before we can process the request.

When a SAR is submitted, we have a duty to provide the information requested within a month, but this can be extended if the request is complicated, or the data cannot be accessed.

When we receive a request, we may ask you to be more specific about the information that you require. This is to refine any queries to make sure we are providing you with the information that you need.

In some cases, we cannot share all information we hold on file if there are contractual, legal or regulatory reasons.

We cannot release information provided by a third party without their consent, and in some cases it may be advisable to approach the third party directly, for example, school nurses who are employed by the NHS.

We will supply the information requested either in paper or electronic form.

If you have any complaints about a SAR, this is covered in our Complaints Policy.

Who is a 'Data Controller'?

Our governing body is the Data Controller. They have ultimate responsibility for how the school manages data. They delegate this to data processors to act on their behalf.

The data controller can also have contracts and agreements in place with outside agencies who are data processors.

Who is a 'Data Processor'?

This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third-party company, possibly a governor, a contractor or temporary employee. It can also be another organisation, such as the police or the Local Authority.

Data Controllers must make sure that Data Processors are as careful about the data as the controller themselves. The UK GDPR places additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.

Processing data

Our school must have a reason to process the data about an individual. Our privacy notices set out how we use data. The UK GDPR has 6 conditions for lawful processing and any time we process data relating to an individual it is within one of those conditions.

The legal basis and authority for collecting and processing data in school are:

- consent obtained from the data subject or their parent.
- performance of a contract where the data subject is a party.
- compliance with a legal obligation.
- to protect the vital interests of the data subject or other associated person.
- to carry out the processing that is in the public interest and/or official authority.
- it is necessary for the legitimate interests of the data controller or third party.
- in accordance with national law.

In addition, any special categories of personal data are processed on the grounds of

- explicit consent from the data subject or about their child.
- necessary to comply with employment rights or obligations.
- protection of the vital interests of the data subject or associated person.
- being necessary to comply with the legitimate activities of the school.
- existing personal data that has been made public by the data subject and is no longer confidential.
- bringing or defending legal claims.
- safeguarding.
- national laws in terms of processing genetic, biometric or health data.

Processing data is recorded within the school systems.

Data Sharing

Data sharing is done within the limits set by the UK GDPR. Guidance from the Department for Education, health, the police, local authorities and other specialist organisations may be used to determine whether data is shared.

The basis for sharing or not sharing data is recorded in school.

Data Breaches & Non Compliance

The school has a separate policy and procedure for dealing with data breaches and once notified of a breach or non-compliance, will take immediate action to remedy the situation as quickly as possible.

We take data protection very seriously and protecting data and maintaining the rights of Data Subjects is the very purpose of this policy and our associated procedures.

Consent

Where required, 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.

Consent is defined by the UK GDPR 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 a 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.

Consent and Renewal

Our privacy notices explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Commented [JW2]: This will depend on how you choose to manage the hosting of information. IDEALLY provide web links to those privacy notices for parents, pupils, common to all and job applicants.

We have privacy notices for pupils, staff, governors, job applicants and for trips and visits. We also have a general privacy notice.

Obtaining clear consent when required and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

For Pupils and Parents/Carers

On joining the school, parents are asked to complete a form advising on next of kin, emergency contact and other essential information. This form is then reviewed by parents on an annual basis. It is important that parents take the time to review this form and advise the school of any changes.

Parents are also asked to complete a permissions form relating to consent relating to the taking of photos and videos, the use of these photos and videos and participation in activities and events taking place in or out of school. This form is only completed once when your child joins school. Consent can be withdrawn at any time, and it is important to inform school if details or your decision about consent changes. It is the obligation of each individual to notify the school of changes.

Pupil Consent Procedure

Where processing relates to a child under 13 years old, school will obtain the consent from a person who has parental responsibility for the child as required.

Pupils may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

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 the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

If you wish to withdraw consent, you will need to contact the school office.

CCTV Policy

We use CCTV and store images for a period of time in line with our CCTV policy.

We use CCTV for the prevention and detection of crimes in the school and the surrounding area.

Data Protection Officer

We have a Data Protection Officer whose role is:

- To inform and advise the controller or the processor and the employees who carry out processing of their obligations under the UK GDPR.
- To monitor compliance with the UK GDPR and DPA.
- To provide advice where requested about the data protection impact assessment and monitor its performance.
- To be the point of contact for Data Subjects if there are concerns about data protection.
- To cooperate with the supervisory authority and manage the breach procedure.
- To advise about training and CPD for the UK GDPR.

Our DPO is John Walker. The contact details for our DPO are:

PHP Law LLP
6 Delamore Park
Cornwood
Ivybridge
PL21 9QP
United Kingdom

Email john.walker@phplaw.co.uk

Physical Security

As a school we are obliged to have appropriate security measures in place.

Every secure area in school has individuals who are responsible for ensuring that the space is securely maintained and controlled if unoccupied, i.e., locked. Offices and cupboards that contain personal data should be secured if the processor is not present.

The headteacher and school business officer are responsible for authorising access to secure areas.

All staff, contractors and third parties who have control over lockable areas must take due care to prevent data breaches.

All sites and locations need to have suitable security and review measures in place.

Secure Disposal

When disposal of items is necessary a suitable process is used. This is to secure the data and to provide a process that does not enable data to be shared in error, by malicious or criminal intent.

These processes, when undertaken by a third party are subject to contractual conditions to

ensure UK GDPR and DPA compliance.

Complaints & the Information Commissioner Office (ICO)

The school's complaint policy deals with complaints about data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked us to erase, rectify, or not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaint procedure.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: casework@ico.org.uk Helpline: 0303 123 1113 web: www.ico.org.uk

Compliance Review

A review of the effectiveness of UK GDPR compliance and processes will be conducted by the Data Protection Officer every 24 months.

Policy Review

This policy was reviewed in May 2023 by the Data Protection Co-ordinator.

This policy was approved for use by the governing body at their meeting on Monday 17 July 2023.

This policy will be reviewed in Summer 2024 in accordance with our policy review schedule.

We will review this policy earlier than the scheduled review date should there be any change in guidance or legislation related to this policy or if we feel that an earlier review is necessary.