

DATA PROTECTION POLICY

STANLEY ST. PETER'S CE (VC) PRIMARY & NURSERY SCHOOL



Approved by: Headteacher

Date: 27/7/26

Last reviewed on: August 2026

Next review due by: August 2027

Document control table			
Document title:		Data Protection Policy	
Author (name & job title):		Michelle Wiggins Headteacher	
Version number:		V4	
Date approved:			
Approved by:		Governors	
Date of next review:		27/7/27	
Document History			
Version	Date	Author	Note of revisions
V2	8/8/24	MWiggins	Document control table added. Clarification added that although a Data Protection Policy is no longer on the list of statutory policies required by the DfE, it is still required by law.
V3	29/7/25	MWiggins	SBM changed to Claire Frier
V4	27/7/26	MWiggins	Updated references to UK GDPR, international transfers, AI guidance, retention arrangements, monitoring requirements and linked policies. Administrative updates and compliance review against ICO guidance.

Contents

1. Overview	3
2. Legislation and guidance	4
3. Definitions	4
4. The Data Controller	5
5. Roles and Responsibilities	5
5.1 Children and Subject Access Requests.....	5
5.2 Responding to Subject Access Requests.....	5
5.3 Children and Subject Access Requests.....	6
5.4 Responding to Subject Access Requests.....	6
6. Data Protection Principles	7
7. Processing Personal Data: Lawfulness, Fairness and Transparency.....	7
8. Processing Special Category Data	9
9. Limitation, Minimisation and Accuracy.....	11
10. Sharing Personal Data.....	11
11. How Personal Data Should be Processed on Behalf of the School	13
12. Data Breaches.....	14
13. Subject Access Requests and Other Rights of Individuals.....	15
13.5 Children and Subject Access Requests.....	16
13.6 Responding to Subject Access Requests.....	16
14. Other Data Protection Rights of the Individual.....	17
15. Parental Requests to see the Educational record	17
16. CCTV	18
17. Photographs and Videos	18
18. Artificial Intelligence (AI).....	18
19. Data Protection by Design and Default	19
20. Data Security and Storage of Records	19
21. Disposal of Records	20
22. Personal Data Breaches	20
23. Training.....	20
24. Monitoring Arrangements.....	21
25. Contacts.....	21
26. Links with Other Policies.....	21

1 Overview

1.1 Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(UK GDPR\)](#) and the Data Protection Act 2018 (hereafter DPA2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.2 The School has a duty to notify staff, Governors and other stakeholders who work for or on behalf of the School, of the information contained in this policy.

1.3 This policy applies to current and former employees, Governors, volunteers, apprentices and consultants. If you fall into one of these categories, then you are a 'data subject' for the purposes of this policy. Please read this policy alongside your contract of employment (or contract for services) and any other notice the School issues from time to time in relation to personal data.

1.4 The School has separate policies and privacy notices in place in respect of job applicants, pupils, parents, suppliers and other categories of data subject. A copy of these can be obtained from the school office or the school website www.stanleystpeters.co.uk

1.5 The School has measures in place to protect the security of personal data in accordance with the Data Security Policy. A copy of the Data Security Policy can be obtained from the school office or the school website www.stanleystpeters.co.uk

1.6 The School will hold data in accordance with its Data Retention Policy. A copy of this can be obtained from our School Business Manager. The School will only hold data for as long as necessary for the purposes for which it was collected.

1.7 The School is a 'Data Controller' for the purposes of processing personal data. This means that the School determines the purpose and means of the processing of personal data.

1.8 This policy explains how the School will hold and process personal data. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the School.

1.9 This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the School at any time.

2 Legislation and Guidance

2.1 This policy meets the requirements of the UK GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and the ICO's [code of practice for subject access requests](#).

2.2 It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

2.3 In addition, this policy complies with regulation 5 of the [Education \(Pupil Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

3 Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable individual on its own, or when taken together with other information likely to come into our possession It includes any expressions of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username
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

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4 The Data Controller

4.1 Our School processes personal data relating to parents, pupils, staff, governors, visitors and others, and is a data controller.

4.2 The School is registered as a Data Controller with the ICO, registration number **Z7303162**, and will renew this registration annually or as otherwise legally required.

4.3 The School delegates the responsibility of the Data Controller to the Data Controller's Representative (See Section 5.2 below)

5 Roles and Responsibilities

This policy applies to **all staff** employed by our School, Governors, volunteers, consultants and to other external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Board

5.1.1 The Governing Board has overall responsibility for ensuring that our School complies with all relevant data protection obligations.

5.2 The Data Controller's Representative

5.2.1 The Headteacher acts as the representative of the Data Controller on a day-to-day basis.

5.2.2 Day-to-day responsibilities rest with the Data Controller's representative, Miss Michelle Wiggins or the Business Manager in their absence.

5.2.3 The Data Controller's representative will ensure that all School staff, Governors and other stakeholders who work for, and on behalf of the School are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

5.3 Data Protection Officer

5.3.1 The Data Protection Officer for the School is Tim Pinto tpinto@esafetyoffice.co.uk

5.3.2 The Data Protection Officer (DPO) is responsible for monitoring our compliance with data protection law and assisting with developing related policies and guidelines where applicable.

5.3.3 The DPO will provide an annual report of their activities directly to the Governing Board and, where relevant, report to the Board their advice and recommendations on School data protection issues.

5.3.4 The DPO is also the first point of contact for individuals whose data the School processes, and for the ICO.

5.4 All Staff

5.4.1 Staff, Governors and other stakeholders who work for or on behalf of the School are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the School of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
 - 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 and before implementing the Data Impact Assessment process
- If they need help with any contracts or sharing personal data with third parties

6. Data Protection Principles

6.1 The UK GDPR is based on data protection principles that our School must comply with.

6.2 The principles say that personal data must be:

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

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

6.3 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data.

6.4 Personal data shall not be transferred outside the UK

6.5 unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

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

7. Processing Personal Data: Lawfulness. Fairness and Transparency

7.1 The School processes data relating to those persons who are employed to work at or are otherwise engaged to work at the School. The purpose of processing this data is to assist in the running of the School. The School will process personal data (including special categories of personal data) in accordance with its obligations under the UK GDPR and the DPA 2018.

Document Control Number:

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

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

7.3 The School can process personal data for these purposes without knowledge or consent. The School will not use personal data for an unrelated purpose without disclosing the intent and providing the legal basis for the processing.

7.4 If the School is not provided with certain personal data, the School may not be able to carry out parts of its contractual obligations. For example, if bank account details are not provided, the School may not be able to pay an employee. It may also prevent the School from complying with certain legal obligations and duties such as paying the right amount of tax to HMRC or making reasonable adjustments in relation to a disability.

7.5 The School must process personal data in various situations during recruitment, employment (or engagement) and even following termination of employment (or engagement). For example:

- Making a decision about your recruitment or appointment;
- Determining the terms on which you work for us;
- Checking you are legally entitled to work in the UK;
- Checking the award of Qualified Teacher Status, completion of teacher induction and prohibitions, sanctions and restrictions that might prevent the individual from taking part in certain activities or working;
- To maintain our single central record and to comply with our general safeguarding obligations;
- To provide information on our website about our staff and Governors;
- Paying you and, if you are an employee, deducting tax and National Insurance contributions;
- Liaising with your pension provider;
- Administering the contract entered into with you;

- In order to operate as a School, which may involve us sharing certain information about our staff with our stakeholders or processing correspondence or other documents, audits or reports which contain your personal data;
- Business management and planning, including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements;
- Making decisions about salary reviews and compensation;
- Assessing qualifications for a particular job or task, including decisions about promotions;
- Gathering evidence for possible grievance or disciplinary hearings;
- Responding to complaints or investigations from stakeholders or our regulators;
- Making decisions about your continued employment or engagement;
- Making arrangements for the termination of our working relationship;
- Providing references to prospective employers;
- Education, training and development requirements;
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Ascertaining your fitness to work;
- Managing sickness absence;
- Complying with health and safety obligations;
- To prevent fraud;
- To monitor your use of our information and communication systems to ensure compliance with our IT policies;
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution;
- To conduct data analysis studies to review and better understand employee retention and attrition rates;
- In connection with the Transfer of Undertaking (Protection of Employment) Regulations 2006, for example, if a service is outsourced or in connection with an academy conversion.
- To maintain and promote equality in the workplace;
- To receive advice from external advisors and consultants;
- In appropriate circumstances to liaise with regulatory bodies, such as the Department for Education, the DBS and the Local Authority about your suitability to work in a School or in connection with other regulatory matters;
- for any other reason which the School is obliged to give notice of, from time to time.

8. Processing Special Category Personal Data

8.1 The School will only process special categories of personal data (see section 3 above for definition), in certain situations and in accordance with the law. For example, if explicit consent has been obtained for the processing. If the School asks for consent to process a special category of personal data, then it will explain the reasons for the request. Consent to process special category data may be refused. If consent is given, it can be withdrawn later by contacting the Business Manager.

8.2 The School does not need consent to process special categories of personal data when it is being processed for the following purposes in accordance with Section 9.2 of the UK GDPR:

- where it is necessary for carrying out rights and obligations under employment law;
- where it is necessary to protect vital interests or those of another person where they are physically or legally incapable of giving consent;
- where the data has been made public, for example through Social Media;
- where processing is necessary for the establishment, exercise or defence of legal claims;
- where processing is necessary for the purposes of occupational medicine or for the assessment of working capacity;

8.3 Examples of Special Category Personal data the School may process include:

- race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- sickness absence, health and medical conditions to monitor absences, assess fitness for work, to pay benefits, for insurance purposes, to comply with legal obligations under employment law including to make reasonable adjustments and to comply with health and safety;
- trade union membership to pay any subscriptions and to comply with legal obligations in respect of trade union members.
- Any other lawful purpose we may inform you of from time to time

8.4 The School may use information relating to criminal convictions where the law allows us to do so. It is envisaged the School will hold information about criminal convictions if information about criminal convictions comes to light as a result of our recruitment and Disclosure and Barring Service checks, or if information about criminal convictions comes to light during your employment with us. Information about criminal convictions and offences will be used in the following ways:

- To ensure employee suitability to work
- For safeguarding purposes

Less commonly, information relating to criminal convictions may be used where necessary in relation to legal claims; where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

8.5 Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. The School may use automated decision-making in the following circumstances:

- Where you have been notified of an automated decision and been given 21 days to request a reconsideration.
- Where it is necessary to meet our obligations under your employment contract and ensure that appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

8.6 If the School makes an automated decision on the basis of any particularly sensitive personal information, it must have either your explicit written consent or it must be justified in the public interest, and it must also put in place appropriate measures to safeguard your rights.

8.7 You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless there is a lawful basis for doing so and you have been notified.

8.8 We do not envisage that any decisions will be taken about you using automated means; however, we will notify you in writing if this position changes.

9 Limitation, Minimisation and Accuracy

9.1 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.

9.2 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.

9.3 Staff must only process personal data where it is necessary in order to do their jobs.

9.4 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for Schools](#).

10. Sharing Personal Data

10.1 Occasionally, we share personal data in order to meet the Schools' contractual obligations, or to meet statutory obligations. For example:

- the Local Authority
- the Department for Education

- the Education & Skills Funding Agency
- the Disclosure and Barring Service
- the Teaching Regulation Agency
- the General Teaching Council for England

10.2 We will also share personal data with law enforcement and other bodies and others where we are legally required to do so, including:

- the Teachers' Pension Service
- HMRC for the assessment and collection of tax
- the Police or other law enforcement agencies for the prevention or detection of crime and/or fraud
- our legal advisors in connection with legal proceedings
- Insurance providers / Risk Protection Arrangement
- [Insert others as necessary/relevant
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils, staff or other stakeholders.

10.3 Other instances where we may share limited personal data include:

- where there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- where we need to liaise with other agencies – we will seek consent as necessary before doing this
- where our third-party 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
 - 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

10.4 The School does not routinely share data with organisations outside the European Economic Area (EEA). Where this may be necessary, e.g. where a former employee has emigrated and/or applied to work outside the EEA, data may be transferred to the new employee with explicit consent from the former employee and with appropriate safeguards.

10.5 We will not transfer personal data outside the EEA unless such transfer complies with the UK GDPR.

This means that we cannot transfer any personal data outside the EEA unless:

- The EU Commission has decided that another country or international organisation ensures an adequate level of protection for personal data
- One of the derogations in the UK GDPR applies (including if an individual explicitly consents to the proposed transfer).

11. How Personal Data Should be Processed on Behalf of the School

11.1 Everyone who works for, or on behalf of, the School has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the School's Data Security and Data Retention policies.

11.2 The School's Data Protection Officer and the Data Controller's Representative are responsible for reviewing this policy and updating the Governing Body on the School's data protection responsibilities and any risks in relation to the processing of data. Any questions in relation to this policy or data protection should be directed to these persons.

11.3 Staff should only access personal data covered by this policy if it is required for the work they do for, or on behalf of the School and only if authorised to do so.

11.4 Staff should only use the data for the specified lawful purpose for which it was obtained.

11.5 Staff should not share personal data informally.

11.6 Staff should keep personal data secure and not share it with unauthorised people.

11.7 Staff should regularly review and update personal data which they have to deal with for work. This includes telling the School if their own contact details change.

11.8 Staff should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

11.9 Staff should use strong passwords.

11.10 Staff should lock computer screens when not at their desks.

Document Control Number:

11.11 Personal data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.

11.12 Personal data should never be transferred outside the UK except in compliance with UK GDPR and the Data Protection Act (2018) and in consultation with the Data Controller's representative and the DPO.

11.13 Staff should not leave paper containing personal data lying about on desks. Storage drawers and filing cabinets should be locked.

11.14 Staff should not take personal data away from School premises without authorisation from their line manager.

11.15 Where possible, paper copies of personal data should be shredded and disposed of securely following transfer to electronic systems. Where hard copy data is retained it should be done so securely.

11.16 Staff should ask for help from the Data Protection Officer/Data Protection Manager if they are unsure about data protection or if they notice any areas of data protection or security that can be improved upon.

11.17 Any deliberate or negligent breach of this policy may result in disciplinary action being taken in accordance with the School's Disciplinary Procedure.

11.18 It is a criminal offence to conceal or destroy personal data which is part of a Subject Access Request (see below). Such conduct would also amount to gross misconduct under the Schools Disciplinary Procedure and could result in dismissal.

12. Data Breaches

12.1 The School has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur, then the School must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then the Information Commissioner's Office must be notified within 72 hours.

12.2 If any staff member is aware of a Data Breach, they must contact their line manager immediately and keep any evidence they have in relation to the breach.

12.3 For further information please refer to the Data Security Policy and Breach Procedure.

13. Subject Access Requests and Other Rights of Individuals

13.1 Subject Access Requests (SARs)

Individuals have a right to make a 'subject access request' to gain access to personal information that the School holds 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 for, 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

13.2 A SAR may be made in writing or verbally, through traditional channels of communication only. If a SAR request is received, it should be forwarded immediately to the Headteacher who will liaise with the Data Protection Officer and coordinate a response.

13.3 A SAR **does not** have to contain the words Subject Access Request. Any communication, whether written or verbal, **that requests access to personal data should be treated as a possible SAR**. Refer to the Subject Access Request Policy and Procedure for further information.

13.4 A form is available to staff, Governors, and other stakeholders who work for or on behalf of the School who wish to make a SAR in relation to their own personal data. Use of the form is not compulsory. The School must accept a SAR in any written or verbal form. The School may, however, contact the requester for further information if necessary. At a minimum, a SAR must contain:

- The requester's full legal name and contact address
- Current email address and telephone number
- Details of the information required.

Please refer to the Subject Access Request Policy and Procedure for further information

13.5 Children and Subject Access Requests

13.5.1 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 on behalf of their child, the child must either:

- be unable to understand their rights and the implications of a subject access request
- have given their consent.

13.5.2 The school will assess a child's capacity to exercise their own information rights on a case-by-case basis. 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.

13.6 Responding to Subject Access Requests

13.6.1 When responding to requests, we:

- may ask the individual to provide 2 forms of identification if we are not confident about the requester's identity
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of a valid Subject Access Request. A request is not considered valid until we have confirmed the identity of the requester and their entitlement to the requested data
- will provide the information free of charge
- 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 any delays as soon as practicable and within 1 month, and explain why the extension is necessary.

13.6.2 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

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

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

13.6.5 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

14. Other Data Protection Rights of the Individual

14.1 In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), 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 UK
- 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)

14.2 Individuals wishing to exercise any of their Data Subject rights should submit a request to their line manager or other appropriate member of staff

14.3 If staff receive such a request, they must immediately forward it to their Line manager, who will liaise with the Data Controller's representative and the DPO.

15 Parental Requests to see the Educational Record

15.1 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.

16. CCTV

16.1 We use CCTV in various locations around the School site to ensure it remains safe. We will adhere to the ICO's Video Surveillance Guidance for the use of CCTV.

16.2 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

16.3 Any enquiries about the CCTV system should be directed to the Headteacher.

17. Photographs and Videos

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

17.2 Staff must not take images of children unless they have:

- A legitimate reason for doing so
- Permission to do so
- Parental/carers consent

17.3 Staff must ensure that written consent has been obtained from parents/carers before photographs and videos are taken of their child and before use of the images in communication, marketing and promotional materials.

17.4 We will clearly explain how the photograph and/or video will be used to both the parent/carers and pupil. Uses may include:

- Within School on notice boards and in School magazines, brochures, newsletters, etc.
- Outside of School by external agencies such as the School photographer, newspapers, campaigns
- Online on our School website or social media pages

17.5 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.

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

17.7 See our Safeguarding and Child Protection Policy for more information on our use of photographs and videos.

18. 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. Stanley St Peter's CE Primary School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

The use of AI by staff and pupils is subject to the school's Online Safety Policy, Acceptable Use Agreements and Filtering and Monitoring arrangements.

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, Stanley St Peter's CE Primary School will treat this as a data breach, and will follow the personal data breach procedure.

Staff must not upload personal, confidential or sensitive school information into AI tools unless the tool has been formally approved by the school and appropriate data protection safeguards are in place.

19. Data Protection by Design and Default

19.1 We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- 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 law (see section 6)
- Completing Data Protection 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 (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting 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

20. Data Security and Storage of Records

20.1 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:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must 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
- Where personal information needs to be taken off site, staff must sign it in and out from the School office (In what form? For what purpose? Safeguards against loss?)

- Passwords that are at least 8 characters long containing letters and numbers are used to access School computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops 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 online safety policy/ICT policy on acceptable use)
- 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 (see section 10)
- Please see the Data Security and Breach Procedure for more information

21. 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.

22. Personal Data Breaches

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

22.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in The Data Security Policy and Breach Procedure

22.3 When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a School context may include, but are not limited to:

- 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

22.4 See the Data Security and Breach Procedure for more information

23. Training

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

Document Control Number:

23.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

24. Monitoring Arrangements

24.1 The Headteacher/Data Controllers Representative, Miss Michelle Wiggins, together with the Data Protection Officer, are responsible for monitoring and reviewing this policy.

24.2 The Headteacher/Data Controllers Representative, Miss Michelle Wiggins, together with the Data Protection Officer, check that the School complies with this policy by, among other things, reviewing School records, policies and procedures annually.

24.3 This policy will be reviewed and updated as and when necessary in relation to any amendments to Data Protection legislation or guidance, or any internal concerns resulting from policy violations, data breaches, or on an annual basis.

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies. This document has now been withdrawn; however, the DfE's latest guidance does not include data protection in its list of statutory policies for maintained schools or academies, including free schools. However, it is a legal requirement that your school/trust has data protection policies and procedures in place.

24.4 At every review, the policy will be shared with the Governing Board.

25. Contacts

25.1 Any questions or concerns about how the School processes personal information or any requests to exercise data protection rights should be submitted to the School in the first instance.

25.2 If the School is not able to address concerns and resolve them satisfactorily, please contact the Data Protection Officer at the address below.

25.3 Finally, concerns can be registered with the UK's data protection regulator, the Information Commissioner's Office, by following this link <https://ico.org.uk/global/contact-us/email/>

25.4 Contact Details:

Data Controller: Stanley St. Peter's CE(VC) Primary & Nursery School, Lake Lock Road, Stanley, WAKEFIELD WF3 4HS

Data Controller's Representative: Miss Michelle Wiggins, Headteacher mwiggins@stanleystpeters.co.uk

Data Protection Manager: Mrs Claire Frier, School Business Manager cfrier@stanleystpeters.co.uk

Data Protection Officer: Tim Pinto tpinto@esafetyoffice.co.uk

26. Links with Other Policies

26.1 This Data Protection Policy is linked to our:

- Freedom of Information policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Data Impact Assessment Policy & Procedure
- Subject Access Request Policy & Procedure
- Data Security Policy and Breach Procedure
- Data Retention Policy
- CCTV Policy