Stamford Green Primary School and Nursery

Data Protection Policy and Privacy Notices

Agreed at:

- Full Governing Body Meeting __
- Children and Learning Committee Meeting __
- Resources Committee Meeting __*

23.6.23

Data Protection Policy and Privacy Notices

Based on model policy from Satswana Ltd last reviewed Sep 2022

Data Protection Policy

1) Aims

a) 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 (GDPR) and statutory guidance.

b) This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2) Legislation and guidance

a) This policy meets the requirements of the GDPR and 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.

b) It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

c) 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, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
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 • Gender
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

a) Our school processes personal data relating to individuals and therefore is a data controller.

b) The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5) Roles and responsibilities

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

b) The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

c) The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

d) The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

e) The school's DPO is Satswana Ltd, info@satswana.com, 01252 516898.

f) The School Business Leader is the Data Protection Manager (DPM) and, along with the Headteacher, acts as the representative of the data controller on a day-to-day basis.

g) All staff are responsible for:

i) Collecting, storing and processing any personal data in accordance with this policy

ii) Informing the school of any changes to their personal data, such as a change of address

iii) Reporting data breaches via the folder in the Headteacher's office

iv) 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
- 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.

6) Data protection principles

a) The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

i) Processed lawfully, fairly and in a transparent manner

ii) Collected for specified, explicit and legitimate purposes

iii) Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

iv) Accurate and, where necessary, kept up to date

v) Kept for no longer than is necessary for the purposes for which it is processed

vi) Processed in a way that ensures it is appropriately secure

7) Collecting personal data

a) Lawfulness, fairness and transparency – the school will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

i) 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.

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

iii) The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.

iv) 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.

v) 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)

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

b) 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.

c) If the school offers online services to pupils, such as classroom apps, and the school intends to rely on consent as a basis for processing, parental consent will be obtained (except for online counselling and preventive services).

d) Whenever the school first collects personal data directly from individuals, the School will provide them with the relevant information required by data protection law.

8) Limitation, minimisation and accuracy

a) The school will only collect personal data for specified, explicit and legitimate reasons. The school will explain these reasons to the individuals when we first collect their data.

b) If the school wants 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.

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

d) 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 school's record retention schedule.

9) Sharing personal data

a) We will not normally share personal data with anyone else, but may do so where:

i) There is an issue with a pupil or parent/carer that puts the safety of our staff at risk.

ii) There is a need to liaise with other agencies.

iii) The school's suppliers or contractors need data to enable the school to provide services to staff and pupils – for example, IT companies. When doing this, the school 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.

b) The school will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

i) The prevention or detection of crime and/or fraud.

ii) The apprehension or prosecution of offenders.

iii) The assessment or collection of tax owed to HMRC.

iv) In connection with legal proceedings.

v) Where the disclosure is required to satisfy our safeguarding obligations.

vi) Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

c) The school may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects pupils or staff.

d) Where the school transfers personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

10) Subject access requests and other rights of individuals

a) Subject access requests

i) 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.

ii) Subject access requests must be submitted in writing, either by letter or email to the DPO or Headteacher. They should include:

- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

iii) If staff receive a subject access request they must immediately forward it to the DPO or Headteacher.

b) Children and subject access requests

i) 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.

ii) Children below the age of 13 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 by the Headteacher.

c) Responding to subject access requests:

i) When responding to requests, the school:

- May ask the individual to provide 2 forms of identification including photo identification.
- May contact the individual via phone to confirm the request was made .
- Will respond without delay and within 1 month of receipt of the request.
- Will provide the information free of charge.
- May tell the individual the school will comply within 3 months of receipt of the request, where a request is complex or voluminous.

b) The school will not disclose information if it:

ii) Might cause serious harm to the physical or mental health of the pupil or another individual.

iii) 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.

iv) Is contained in adoption or parental order records.

v) Is given to a court in proceedings concerning the child.

d) 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.

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

f) When the school refuses a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

11) Other data protection rights of the individual

a) 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:

i) Withdraw their consent to processing at any time.

ii) Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).

iii) Prevent use of their personal data for direct marketing.

iv) Challenge processing which has been justified on the basis of public interest.

v) Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

vi) Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them).

vii) Prevent processing that is likely to cause damage or distress.

viii) Be notified of a data breach in certain circumstances.

ix) Make a complaint to the ICO.

x) Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

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

12) Parental requests to see the educational record

a) 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.

13) CCTV

a) The school uses CCTV at the West Gate to ensure the school site remains safe. No recordings are made. Any enquiries about the CCTV system should be directed to the School Business Leader in the first instance.

14) Photographs and videos

a) As part of our school activities, we may take photographs and record images of individuals within the school.

b) The school will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

c) Uses may include:

   i) Within school on notice boards and in school magazines, brochures, newsletters, etc.

   ii) Outside of school by external agencies such as the school photographer, newspapers, campaigns.

   iii) Online on our school website or social media pages.

d) 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.

e) 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.

15) Data protection by design and default

a) The school will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

   i) Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

   ii) 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 7).

   iii) Completing 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 (the DPO will advise on this process).

   iv) Integrating data protection into internal documents including this policy, any related policies and privacy notices.

v) 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.

vi) Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

vii) 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

a) The school 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.

b) In particular:

i) 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.

ii) Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else, such as notice boards, where there is general access to non-staff members.

iii) Personal information should only be taken off site if absolutely necessary and staff must adhere to procedures in the Staff Code of Conduct to keep information safe and secure.

c) Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.

d) Personal data is not stored locally on any laptops or other portable devices. USB devices are not allowed in school.

e) Staff, pupils and governors are not allowed to store personal information on personal devices.

f) 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 9).

17) Disposal of records

a) 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.

b) Paper based records will be shredded and electronic files will be deleted. The school 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.

18) Personal data breaches

a) The school will make all reasonable endeavours to ensure that there are no personal data breaches.

b) In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

c) 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:

   i) A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium.

   ii) Safeguarding information being made available to an unauthorised person.

   iii) The theft of a school laptop containing non-encrypted personal data about pupils.

19) Training

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

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

20) Monitoring arrangements

a) The Data Protection Officer is responsible for monitoring and reviewing this policy.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1) On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPM. If the breach is considered serious in nature, the DPM will contact the DPO.
2) The DPM will seek advice from the DPO as necessary and will investigate the report, and determine whether a breach has occurred. To decide, the DPM will consider whether personal data has been accidentally or unlawfully:
    a) Lost
    b) Stolen
    c) Destroyed
    d) Altered
    e) Disclosed or made available where it should not have been
    f) Made available to unauthorised people
3) The DPM will alert the Headteacher and chair of governors
4) The DPM will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
5) The DPM will assess the potential consequences, based on how serious they are, and how likely they are to happen
6) The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    a) Loss of control over their data
    b) Discrimination
    c) Identify theft or fraud
    d) Financial loss
    e) Unauthorised reversal of pseudonymisation (for example, key-coding)
    f) Damage to reputation
    g) Loss of confidentiality
    h) Any other significant economic or social disadvantage to the individual(s) concerned

    If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
7) The Headteacher / SBL will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the data breach folder in the Headteacher's office.
8) Where the ICO must be notified, the DPM will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPM will set out:
    a) A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned

b) The name and contact details of the DPO

c) A description of the likely consequences of the personal data breach

d) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

9) If all the above details are not yet known, the DPM will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPM expects to have further information. The DPM will submit the remaining information as soon as possible

10) The DPM will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPM will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

a) The name and contact details of the DPO

b) A description of the likely consequences of the personal data breach

c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

11) The DPM will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

12) The DPM will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

e) Facts and cause

f) Effects

g) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the data breach folder in the Headteacher's Office.

The DPO and DPM will review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

1) If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

2) Members of staff who receive personal data sent in error must alert the sender and the DPM as soon as they become aware of the error

3) If the sender is unavailable or cannot recall the email for any reason, the DPM will ask the ICT department to recall it
4) In any cases where the recall is unsuccessful, the DPM will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
5) The DPM will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
6) The DPM will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

7) Other types of breach could include:

Sensitive information being disclosed in hard copy (for example a school report being sent to the wrong parents / carers)

1) Details of pupil premium interventions for named children being published on the school website
2) Non-anonymised pupil exam results or staff pay information being shared with governors
3) A school laptop containing non-encrypted sensitive personal data being stolen or hacked
4) The school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 - Privacy Notice
How we use pupil information

1. The categories of pupil information that we collect, hold and share include:

a) Personal information (such as name, unique pupil number and address).
b) Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility).
c) Attendance information (such as sessions attended, number of absences and absence reasons).
d) Assessment information.
e) Relevant medical information.
f) SEND information.
g) Behavioural/exclusion information.
h) Pastoral information.

2. Why we collect and use this information

We use the pupil data:

a) to support pupil learning;
b) to monitor and report on pupil progress;
c) to provide appropriate pastoral care;
d) to assess the quality of our services;
e) to comply with the law regarding data sharing;

3. The lawful basis on which we use this information

On 25 May 2018 the Data Protection Act 1998 was replaced by the General Data Protection Regulation (GDPR). The conditions for processing under the GDPR are:

Article 6

1. *Processing shall be lawful only if and to the extent that at least one of the following applies:*

(c) Processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 9

1. *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*
2. *Paragraph 1 shall not apply if one of the following applies:*

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union

or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The Education Act 1996 - Section 537A – states that we provide individual pupil information to the relevant body such as the Department for Education.

Children's Act 1989 – Section 83 – places a duty on the Secretary of State or others to conduct research.

4. Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

5. Storing pupil data

We hold pupil data for as long as we need to in order to educate and look after you. We will keep some information after you have left the school, for example, so that we can find out what happened if you make a complaint.

In exceptional circumstances we may keep your information for a longer time than usual, but we would only do so if we had a good reason and only if we are allowed to do so under the law.

We can keep information about you for a very long time or even indefinitely if we need this for historical, research or statistical purposes. For example, if we consider the information might be useful if someone wanted to write a book about the school. Please see our Information and Records Retention Policy for more detailed information.

6. Who we share pupil information with

We routinely share pupil information with:

a) schools that pupils attend after leaving us;
b) our Local Authority (Surrey County Council);
c) the Department for Education (DfE);
d) medical practitioners and NHS staff;
e) agencies involved in caring for and supporting pupils;
f) parents and carers;
g) our catering company – Accent Catering Ltd;
h) our school photographer – Nik Bartrum Photography;
i) external suppliers (e.g. travel companies or those providing off-site activities);
j) curriculum support providers (e.g. Insight, PEBS, Wonde, ScoPay, SIMS).

7. Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the DfE on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the DfE under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

8. Data collection requirements:

a) To find out more about the data collection requirements placed on us by the DfE (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

b) The National Pupil Database (NPD)

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The DfE may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the DfE has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

9. Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs English – PA to the Headteacher via email. pa@stamford-green.surrey.sch.uk .

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

10. Contact

If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer Contact Details	
Name	Satswana Ltd
Email Address	info@satswana.com
Telephone Number	01252 516898
Postal Address	Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

Appendix 3 - School Workforce Privacy Notice

The purpose of this privacy notice is to explain to you the data we collect about you as part of your employment relationship, or other work engagement, with the school.

1. **Name of Data Controller:**

   Stamford Green Primary School and Nursery, Christ Church Mount, Epsom, Surrey, KT19 8LU

2. **Name of our Data Protection Officer:**

   Satswana Ltd, Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH.

3. **What information do we collect about our workforce and how?**

   The categories of school workforce information that we collect, process, hold and share include:

   a) personal information (such as name, contact details for you and your emergency contacts, employee or teacher number, bank account, national insurance number, evidence of your right to work);

   b) special categories of data (including information about your ethnic origin and health conditions);

   c) contract information (such as start dates, hours worked, post, roles and salary information);

   d) work attendance and absence information (such as your work pattern history, number of absences and reasons);

   e) work performance and history (such as appraisal reports and correspondence, information about disciplinary or grievance matters, including any warnings issued to you);

   f) information from your application form and recruitment process, such as qualifications, employment history and pre-employment checks (for example, health assessments and DBS checks);

   g) data from our IT systems which records your use of the internet and work email account;

   h) staff photos;

   i) declarations of interest;

   j) We collect information from you both prior to and during your employment from a range of sources, including your application form, correspondence with you, forms you complete prior to and during employment, from interviews, appraisals and other meetings.

4. **Why we collect and process this information**

   a) We process this information because the processing is necessary for us to enter into an employment (or other work-related) contract with you and for the subsequent performance of that contract, for example to ensure you are paid correctly and receive your entitlements to sick pay and annual leave. We also need to process this

information to ensure that we are complying with our legal obligations, such as ensuring that you have the right to work in the UK, and to defend legal claims.

b) We process special category data, such as information about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations (such as obtaining advice from occupational health providers about health conditions to ensure compliance with employment and health and safety law). Where we process information for the purposes of equal opportunities monitoring, this information is collected only with the express consent of employees. Consent may be withdrawn by an employee at any time.

c) We use other school workforce data to manage the day-to-day operation of the school, where processing is necessary for the purposes of the legitimate interests of the employer. In relying on legitimate interests, we first consider the necessity of processing the data when balanced against the interests, rights and freedoms of the individual. These legitimate interests include:

i. to manage recruitment processes and respond to reference requests;

ii. to inform the development of recruitment and retention policies;

iii. to keep records of employee performance and work history, including training and appraisal records, to ensure acceptable standards of conduct are maintained and to manage training and career progression;

iv. to manage absence effectively;

v. to manage day-to-day HR administration;

vi. to enable the development of a comprehensive picture of the workforce and how it is deployed;

d) We do not make employment decisions based on automated decision-making.

e) If we wish to process your personal data for a new purpose we will inform you of any additional processing.

5. Collecting this information

a) Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

6. Who we share this information with and why

b) Your information will be shared with school staff with an HR or recruitment responsibility and managers within your area of work or department.

c) We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

d) Beyond the school, we share your information when necessary with the local authority, in order to comply with legal obligations and statutory guidance regarding the safeguarding of children and young people.

e) We also share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment of educational attainment. See the section below on 'Department for Education data collection requirements' for further details.

f) Other third parties - we will also share your data with certain third parties to fulfil legal requirements, obtain or provide necessary information or because the third party processes data on our behalf. These third parties include:

   i. your previous employers in order to undertake pre-employment checks;

   ii. the Disclosure and Barring Service in order to undertake pre-employment checks and follow-up checks during employment;

   iii. suppliers and consultants that provide us with a service, such as occupational health, HR or legal services;

   iv. trade unions or any other representative acting on your behalf;

   v. Ofsted.

g) When we appoint third parties to process data on our behalf, the third party is also required to process the data lawfully and fairly and in a manner that ensures appropriate security of the data, using appropriate technical or organisational measures to protect against unauthorised or unlawful processing and accidental loss.

h) We do not transfer your data to countries outside the European Economic Area.

7. Department for Education Data Collection Requirements

a) The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

b) To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

c) The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

   i. conducting research or analysis

   ii. producing statistics

   iii. providing information, advice or guidance

d) The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

   i. who is requesting the data;

   ii. the purpose for which it is required;

   iii. the level and sensitivity of data requested;

   iv. the arrangements in place to securely store and handle the data.

e) To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

f) For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

g) **To contact the department: https://www.gov.uk/contact-dfe**

8. Requesting access to your personal data and your rights as a data subject

a) Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our Data Protection Officer.

b) You also have the right to:

i. object to processing where we are relying on legitimate interests as the legal basis for processing;

ii. in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and

iii. object to decisions being taken by automated means.

c) If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

9. Contact

a) If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer Contact Details	
Name	Satswana Ltd
Email Address	info@satswana.com
Telephone Number	01252 516898
Postal Address	Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

Appendix 4 - Privacy Notice for Job Applicants

The purpose of this privacy notice is to explain to you the data we collect about job applicants as part of our recruitment and selection process.

1. **Name of data controller:**

   Stamford Green Primary School, Christ Church Mount, Epsom, Surrey, KT19 8LU

2. **Name of our data protection officer:**

   Satswana Ltd, Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH.

3. **What information do we collect about job applicants and how?**

   a) The categories of information that we collect, process, hold and share include:

      i. personal information (such as name, date of birth, contact details, National Insurance number, teacher number (if applicable));

      ii. education history and details of qualifications and relevant professional development;

      iii. membership of professional bodies;

      iv. employment history (including any gaps in employment and/or education/training);

      v. information about any reasonable adjustments we need to make to the shortlisting or interview and assessment process to accommodate a disability;

      vi. information about any cautions, convictions, reprimands or final warnings which are not protected, as defined by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended) as well as any current police investigations or pending criminal proceedings;

      vii. information about any disqualification or sanction imposed by a regulatory body in relation to working with children;

      viii. information about your registration with the Disclosure and Barring Update Service (if applicable);

      ix. information about any close personal relationships you may have with an existing member of staff or member of the Board of Governors;

      x. proof of your identity, if invited for interview;

      xi. special categories of data (including information about your ethnic origin and health conditions) in order for us to monitor the success of our equality policies.

   b) We collect information from your application form and, if shortlisted for interview, as part of our selection process which generally includes an interview and some other form of assessment, such as written tests and presentations.

   c) It is our policy, in line with the Department for Education's (DfE) statutory guidance, Keeping Children Safe in Education, to request references at the shortlisting stage, in advance of interview. If you have concerns about this, you should contact us before submitting your application. If you are shortlisted, we will therefore also collect personal data about you from your nominated referees. Personal data may also be collected from other previous employers listed on your application form, for example to verify details on your application form, such as particular experience or qualifications.

d) If an offer of employment is made to you, the offer will be subject to completion of a range of pre-employment checks to our satisfaction, including a criminal records check with the Disclosure and Barring Service and a pre-employment health assessment. You will be informed of the checks to be undertaken in the event that an offer is made.

4. Why we collect and use this information

a) We process data from job applicants in order to undertake the recruitment process and, for the successful applicant, to enter into a contract of employment. In particular it is used to:

i. administer the application, shortlisting and selection process;

ii. assess your suitability to work with children and young people;

iii. inform the development of recruitment and retention policies;

iv. defend legal claims;

v. monitor protected characteristics in order to promote equality at work.

vi. We do not make recruitment decisions based on automated decision-making.

5. The lawful basis on which we process this information

a) We process this information about you because the processing is necessary for us to enter into an employment (or other work-related) contract with you. We also need to process this information to ensure that we are complying with our legal obligations and in particular with the DfE statutory guidance document, Keeping Children Safe in Education, such as by carrying out pre-employment checks on your right to work in the UK and with the Disclosure and Barring Service.

b) We have a legitimate interest in processing data from job applicants in order to administer the recruitment process, to monitor compliance with our policies, to defend any legal claims and to ensure that the most suitable applicant is appointed to the role, based on an assessment of their likely performance amongst other factors. We do not rely on legitimate interests as a reason for processing data unless we have first considered the rights and freedoms of the individuals affected and determined that these do not override the interests we have identified.

c) We process special category data, such as information about your ethnic origin or health, as part of our equal opportunities monitoring process and in order to meet legal obligations (such as the requirement to make reasonable adjustments for job applicants with a disability). This information is collected with the express consent of job applicants. Consent may be withdrawn by an applicant at any time.

d) We may offer to contact unsuccessful applicants within a period of six months following the application if another suitable vacancy arises. Information is only used in this way with the express consent of applicants, which may be withdrawn at any time.

e) If we wish to process your personal data for a new purpose we will inform you of any additional processing.

6. Collecting this information

a) Personal data provided to us as part of the recruitment and selection process is generally given on a voluntary basis and, as such, you have a choice as to whether you provide information to us. However, failure to provide information may mean that your application cannot be processed. You should also be aware that providing false or misleading information (including by omission) may result in your application being rejected and could also be treated as a disciplinary offence in the event that employment is subsequently offered to you.

b) Posts in our organisation are exempt from the Rehabilitation of Offenders Act 1974 (as amended). If you decide to submit an application form, you must disclose any cautions and convictions, even if they are spent, other than protected cautions and convictions (i.e. those which have been filtered out). Details on the filtering rules applicable to certain offences can be found on the Gov.uk website: https://www.gov.uk/government/collections/dbs-filtering-guidance.

c) Equality monitoring information is undertaken only for the purposes of evaluating our equality policies. It is not mandatory and its provision or otherwise will have no effect on the processing of your application form.

7. Storing this information

a) Information from your application form and from the shortlisting and selection process will be stored in a paper-based file, in electronic records within our HR system and also in other IT systems, including email.

b) A copy of your application form and all other personal data collected during the recruitment and selection process will be held as follows:

   i. for successful applicants this will be transferred to a personnel file where it will be held securely. You will be given a workforce privacy notice upon appointment which will explain how we will hold and process your data as an employee;

   ii. for unsuccessful applicants, securely for a period of six months.

8. Who we share this information with and why

a) Your information will be shared with school staff with a recruitment responsibility. This will include members of our HR and administrative staff, those responsible for shortlisting and interviewing and managers within the relevant area of work or department. Equality monitoring information is separated from the application form upon receipt and is not shared with those responsible for shortlisting and interviewing.

b) We do not share information about job applicants with anyone without consent unless the law and our policies allow us to do so.

c) We will not share your data with third parties unless and until an offer of employment is made to you. At that stage, your data will be shared to fulfil legal requirements, obtain or provide necessary information or because the third party processes data on our behalf. These third parties include:

i. the Disclosure and Barring Service in order to undertake a criminal record check;

ii. suppliers and consultants that provide us with a service, such as occupational health, HR or legal services;

iii. relevant professional bodies in order to verify your qualifications (such as the Teaching Regulation Agency for teaching posts).

a) When we appoint third parties to process data on our behalf, the third party is also required to process the data lawfully and fairly and in a manner that ensures appropriate security of the data, using appropriate technical or organisational measures to protect against unauthorised or unlawful processing and accidental loss.

b) We do not transfer your data to countries outside the European Economic Area.

9. Requesting access to your personal data and your rights as a data subject

a) Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our data protection officer (details at the beginning of this document).

b) You also have the right to:

i. restrict processing of your data in certain circumstances;

ii. prevent processing for the purpose of direct marketing;

iii. object to decisions being taken by automated means;

iv. object to the processing of your data where we are relying on our legitimate interests as the lawful basis for processing;

v. in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and

vi. claim compensation for damages caused by a breach of data protection legislation.

c) If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

10. Contact

d) If you would like to discuss anything in this privacy notice, please contact our Data Protection Officer:

Data Protection Officer Contact Details	
Name	Satswana Ltd
Email Address	info@satswana.com
Telephone Number	01252 516898
Postal Address	Pembroke House, St Christopher's Place, Farnborough, Hampshire, GU14 0NH

Appendix 5 – Information and Records Retention Schedule

This schedule lays out the normal retention periods we adhere to. The schedule is based on the IRMS toolkit for schools and advice from HR advisors, adapted for the school's specific requirements. We process data in accordance with data protection principles and data is securely destroyed when it is no longer required.

	Description	Retention Period
1.	**Child Protection**	
a.	Child Protection files	DOB + 25 years[1]
b.	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer
2.	**Governance**	
a.	Minutes:	
i.	Principal set (signed)	Permanent
ii.	Inspection copies	Date of meeting + 3 years
b.	Agendas	Date of meeting
c.	Reports	Date of report+6years
d.	Instruments of Government	Permanent
e.	Action plans	Date of action plan + 3 years
f.	Policy documents	Expiry of policy
g.	Complaints files	Date of resolution of complaint + 6 years
3.	**Management**	
a.	Minutes of the LMT and other internal administrative bodies	Date of meeting + 5 years
b.	Reports made by the Headteacher or LMT	Date of meeting + 5 years
c.	Correspondence created by Headteacher, LMT, ELT and other members of staff with administrative responsibilities	Date of correspondence + 3 years
d.	Professional Development Plan	Closure + 6 years
e.	School Success Plans	Closure + 6 years
f.	Admissions – if the admission is successful	Admission + 1 year
g.	Admissions – if the appeal is unsuccessful	Resolution of case + 1 year
h.	Proof of address supplied by parents as part	Current year + 1 year

	Description	Retention Period
	of the admission process	
i.	Data Collection Forms – paper copy	Disposal after entry into SIMS
4.	**Pupils**	
a.	Electronic attendance registers	Date of register + 7 years
b.	Pupil files retained in school	Transfer to new school when pupil leaves
c.	SEND files, reviews and IEPs	DoB of the pupil + 25 years
d.	Correspondence relating to authorised absence and issues	Date of absence + 2 years
e.	Progress and achievement records (including external testing results)	Current year + 7 years
f.	Any other records created in the course of contact with pupils	Current year + 3 years
g.	Statement maintained under The Education Act 1996 – Section 324	DoB + 30 years
h.	Advice and information to parents regarding education needs	Closure + 12 years
i.	Accessibility strategy	Closure + 12 years
j.	Permission information for school trips where there has been no major incident	Conclusion of the trip
k.	Permission information for school trips where there has been a major incident	DoB of the pupil(s) involved in the incident + 25 years (retain all permissions for the trip not just the affected pupil(s))
l.	Records created by school to obtain approval to run an Educational Visit outside the classroom	Date of visit + 14 years
5.	**Curriculum**	
a.	School Success Plan	Current year + 6 years
b.	Curriculum Returns	Current year + 3 years
c.	Schemes of work	Current year + 1 year (or review and allocate a new retention period if appropriate)
d.	Timetables	Current year + 1 year (or review and allocate a new retention period if appropriate)
e.	Class record books	Current year + 1 year (or review and allocate a new retention period if appropriate)

	Description	Retention Period
f.	Mark books	Current year + 1 year (or review and allocate a new retention period if appropriate)
g.	Record of homework set	Current year + 1 year (or review and allocate a new retention period if appropriate)
h.	Pupils work	Current year + 1 year (or review and allocate a new retention period if appropriate). Golden books are retained for the duration that the pupil is at the school after which they are sent home.
i.	SATS records – examination papers and results	Current year + 6 years
j.	PAN reports	Current year + 6 years
k.	Value added & contextual data	Current year + 6 years
l.	Self Evaluation Forms	Current year + 6 years
6.	**HR**	
a.	Application forms and interview notes: unsuccessful applicants	Date of interview + 6 months
b.	Application forms and interview notes: successful applicants	End of employment + 6 years
c.	Right to Work in the UK checks (in accordance with the Home Office List A and List B)	End of employment + 2 years
d.	Proof of identity for DBS check purposes	Until the results of the DBS check has been received
e.	Details about criminal convictions supplied during the recruitment process	Until recruitment decision has been made. A summary of the risk assessment decision to be retained on file for successful candidates.
f.	DBS check certificates	Until recruitment decision has been made or in any event no later than 6 months from the issue date of disclosure
g.	Proof of qualifications	End of employment + 6 years
h.	Parental leave records	Until the relevant child is 18
i.	Contracts of employment, contract amendment letters, change of pay forms	End of employment + 6 years

	Description	Retention Period
j.	Redundancy details and calculations	End of employment + 6 years
k.	Timesheet/sick pay	Current year + 6 years
l.	Disciplinary records (see also allegations of a child protection nature, below)	End of employment + 6 years
m.	Allegations of a child protection nature against a member of staff	Until the person's normal retirement age, or 10 years from the date of the allegation if longer. Copy of information retained to be given to individual. Details of allegations that are found to be malicious will be removed from personnel records.
n.	Appraisal and training records	End of employment + 6 years
o.	Staff personal files	End of employment + 6 years
p.	Statutory Maternity Pay, Paternity Pay and Adoption Pay records, calculations, certificates (e.g. MAT B1s) or other medical evidence	3 years after the end of the tax year in which the payments were made
q.	Statutory Sick Pay records, calculations, certificates and self-certificates	3 years after the end of the tax year to which they relate
r.	Wage/salary records (including records of overtime, bonuses and expenses)	6 years
7.	**Health and Safety**	
a.	Accessibility Plans	Current year + 6 years
b.	Accident reporting:	
i.	Adults	Date of incident + 7 years
ii.	Children	DoB of child + 25 years
c.	COSHH	Current year + 10 years (or longer if appropriate)
d.	Incident reports	Current year + 20 years
e.	Policy Statements	Date of expiry + 1 year
f.	Risk assessments	Current year + 3 years
g.	Fire log books	Current year + 6 years
8.	**Administrative**	
a.	Letters to staff/parents/pupils	Current year + 1 year
b.	Newsletters	Permanent – as a record of school history
c.	Visitors books	Current year + 2 years

Description	Retention Period
d. PTA	Current year + 6 years
9. Finance	
a. Annual accounts including invoices, receipts and other records.	Current year + 6 years
b. Loans and grants	Date of last payment + 12 years
c. Contracts:	
i. Under seal	Contact completion date + 12 years
ii. Under signature	Contract completion date + 6 years
iii. Monitoring records	Current year + 2 years
d. Budget reports, monitoring etc.	Current year + 3 years
e. Annual budget and background papers	Current year + 6 years
f. Order books & requisitions	Current year + 6 years
g. Delivery documentation	Current year + 6 years
h. Debtors records	Current year + 6 years
i. School fund – cheque books	Current year + 3 years
j. School fund – accounts, paying in books, ledger, invoices, receipts and bank statements	Current year + 6 years then review
k. Free school meal registers	Current year + 6 years
l. Petty cash books	Current year + 6 years
10. Property	
a. Title deeds	Permanent
b. Plans	Permanent
c. Maintenance and contractors	Current year + 6 years
d. Leases	Expiry of lease + 6 years
e. Lettings	Current year + 3 years
f. Burglary, theft and vandalism report forms	Current year + 6 years
g. Maintenance log books	Current year + 6 years
h. Contractors reports	Current year + 6 years then review
11. Local Authority	
a. Secondary transfer sheets	Current year + 2 years
b. Attendance returns	Current year + 1 year

Description	Retention Period
c. Other returns	Current year + 6 years
12. School Meals	
a. Dinner register	Current year + 3 years
b. School meals summary sheets	Current year + 3 years