

# Stanburn Primary School



## Data Protection Policy

<b>Committee Responsible:</b>	<b>Full Governing Body</b>
<b>Review Date:</b>	<b>March 2025</b>
<b>Reviewed By: (Committee Name)</b>	<b>Full Governing Body</b>
<b>Next Review Date:</b>	<b>March 2026</b>
<b>Author:</b>	<b>Monica Cozma</b>

## Contents

Section	Section Title	Page
1	Aims	3
2	Legislation and guidance	3
3	The Data Controller	3
4	Roles and Responsibilities	3
5	Data Protection Principles	4
6	Collecting and Processing Personal Data	4
7	Sharing Personal Data	5
8	Images used by the school	6
9	CCTV	7
10	Staff	7
11	Accuracy of Personal Data	7
12	Data Security and Storage of Records	8
13	Retention of Data and Disposal of Records	8
14	Subject Access Requests and other rights of individuals	9
15	Parental Requests to see the Educational Record	11
16	Training	11
17	Monitoring Arrangements	11

## Appendices

Ref	Appendix Title	Page
A	Definitions	12
B	Roles and Responsibilities	13
C	Data Administrator Confidentiality Agreement	14
D	Data Collection Sheet	15
E	Photo Consent Form	16-17
F	S.A.R Request Form	18-23
G	S.A.R. Release Letter	24
H	Disposal Log/Timeline	25
I	Privacy Notice – Pupils and Parents	26-30
J	Privacy Notice - Staff	31-37

## 1. Aims

Throughout this document, we refer to Data Protection Legislation, which means the Data Protection Act 2018 (DPA2018), the United Kingdom General Data Protection Regulation (UK GDPR), the Privacy and Electronic Communications (EC Directive) Regulations 2003, and any legislation implemented in connection with the aforementioned legislation. Where data is processed by a controller or processor established in the United Kingdom or comprises the data of individuals in the United Kingdom, it is governed by the UK GDPR. Any reference to EU GDPR is no longer applicable since the UK has exited the European Union, and the UK GDPR now governs data protection. This includes any replacement legislation coming into effect from time to time.

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 UK GDPR and the Data Protection Act 2018 (DPA 2018).

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

## 2. Legislation and Guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#). It also reflects the ICO's [code of practice for the use of surveillance cameras](#) and personal information. 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. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 4. Roles and responsibilities

The governing board has overall responsibility for ensuring that the school complies with its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

Day-to-day responsibilities rest with the Headteacher and/or the School Business Manager. The Headteacher will ensure that all staff are aware of their data protection obligations and oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address. 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.

See Appendix B for Roles and Responsibilities of the Data Protection Officer and the Data Protection Coordinator.

## 4.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations under the UK GDPR and the Data Protection Act 2018 (DPA 2018). The board is responsible for ensuring adequate resources and support are allocated for the implementation of this policy.

## 4.2 Data protection officer

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. They will provide an annual report of their activities directly to the governing board and, where relevant, report their advice and recommendations on school data protection issues. The DPO also serves as the first point of contact for individuals whose data the school processes and for the Information Commissioner's Office (ICO).

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is The DPO Centre, and they can be contacted at [advice@dpocentre.com](mailto:advice@dpocentre.com).

## 4.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis, ensuring compliance with data protection regulations across school operations.

## 4.4 All staff

All staff members 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 concerns that this policy is not being followed.
  - If they are unsure whether 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, handle data protection rights invoked by an individual, or transfer personal data outside the UK.
  - If there has been a data breach.
  - Whenever engaging in a new activity that may affect the privacy rights of individuals.
  - If they need assistance with any contracts or sharing personal data with third parties.

## 5. Data Protection Principles

The Data Protection Act 2018 is based on data protection principles that our school must comply with.

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. Collecting and Processing Personal Data

Processing of personal data includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data. Processing also includes transferring data to 3rd parties. (See Appendix A: Definitions)

All forms used by the school to collect personal data about a pupil will carry a standard Data Protection notice: as follows:

*'I/We consent to the school (through the head as the person responsible) obtaining, using, holding and disclosing "Personal data" including "sensitive personal data" (such as medical information), for the purposes of safeguarding and promoting the welfare of our child, and where necessary, for the legitimate interests of the School and ensuring that all relevant legal obligations of the school and ourselves are complied with.*

*I/ We give my/our consent to such processing and disclosure provided that at all times any processing or disclosure of personal data or sensitive personal data is done lawfully and fairly in accordance with the Data Protection Act 2018.'*

### 6.1 Lawfulness, fairness and transparency

We will only process 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 for special categories of personal data; we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

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

### 6.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. 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 Records Management Policy.

## 7. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- 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

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

### **7.1 Disclosure of personal data to third parties**

The school may receive requests from third parties (i.e. those other than the data subject, the school, and employees of the school) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless one of the specific exemptions under the DPA which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the school.

The following are the most usual reasons that the school may have for passing personal data to third parties. To:

- Give a confidential reference relating to a pupil;
- Publish the results of public examinations or other achievements of pupils of the school;
- Disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- Provide information to another educational establishment to which a pupil is transferring;
- Provide the relevant information to the Government Department e.g. DfES, Ofsted, concerned with national education.

The Department for Education uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole.

The statistics are used in such a way that individual pupils cannot be identified from them.

Any wish to limit or object to any use of personal data by third parties, except as stated above, should be notified to the Data Protection Coordinator of the relevant school in writing.

Where the school receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure. When members of staff receive enquiries from third parties for personal data, the enquirer should be asked why the information is required. If consent to the disclosure has not been given (and an exception does not apply) then the request should be declined.

In normal circumstances information should not be disclosed over the phone to third parties. In most circumstances third parties should be asked to provide documentary evidence to support data requests.

## 8. Images used by the school

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

Uses may include:

- Within school on notice boards and in school newsletters/books/emails
- Outside of school by external agencies such as the school photographer, newspapers
- Online on our school website/Class DoJo or Learning Platforms

Consent is given at admission, but it can be refused or withdrawn at any time. If a parent wishes to change their level of consent they should complete a new form and return it the school office to inform the school of the change. If consent is withdrawn, we will delete the photograph or video and not distribute it further. 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.

See our Online Safety and Acceptable Use Policy and our Child Protection Policy for more information on our use of photographs and videos.

## 9. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

Any enquiries about the CCTV system should be directed to the – Site Supervisor. See CCTV policy for further details.

## 10. Staff

The principles of the Data Protection act described in this policy also apply to staff data held in school.

- Staff is made aware of, and agree to their data being processed by signing their contract of employment.
- Sensitive personal data will only be used by the school for legitimate business, management and school purposes and will not be transferred to third parties without consent.
- Staff data will be held securely in locked cabinets or password protected electronic formats. Stanburn Primary school data protection policy will also apply to staff data.
- Use of staff records will be limited to those personnel appointed by the Headteacher as appropriate for specific purposes.

As with all data subjects, staff may request to see, or have a copy of their record under the Subject Access Request provision of the Data Protection Act. If a full copy of the record is requested, Stanburn School has 30 days to respond fully if required. Subject Access Requests should be made to the Headteacher. The exemptions listed earlier in this policy apply.

Staff records will normally be kept for 7 years after their employment has ceased. Unsuccessful applicants will have their data kept for 6 months after their application.

The Data Protection co-ordinator will address the retention periods in the annual audit. They will also remind appropriate staff of the requirement to dispose of expired data securely.

DBS checks are carried out routinely. Staff Records (Single Central Record) will only indicate whether a satisfactory or unsatisfactory check has been received and the date processed. No additional details regarding the DBS check will be held on the staff record.

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school. Further details can be found in the Privacy Notice – Staff (Appendix J).

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact The HR Officer/Headteacher.

## **11. Accuracy of Personal Data**

The school will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the relevant school's Data Protection Coordinator in writing of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected.

Schools will issue a Data Collection Sheet (Appendix D) to all parents/guardians on an annual basis to help with data accuracy.

## **12. Data security and storage of records**

The school will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons. 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 securely 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, it must be kept securely
  - All passwords are set by LGfL and these are used to access school computers, laptops and the school email system. The viewing of passwords is only available to nominated contacts who have a USO-OTP (One Time Password) Second Factor Authentication Device.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB device
- Staff who have access to add, amend and delete personal information will sign and adhere to the Data Administrator Confidentiality Agreement. (See Appendix C)
- Staff and governors do not use personal equipment to store personal information
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

All staff should be aware of the Acceptable Use Policy.



## 13. Retention of Data and 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 or incinerate 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.

The school will not keep pupil and related data for longer than necessary. Records of Primary school pupils will be transferred securely to the next school. Any records or part of records retained will be disposed of 7 years after the pupil finishes their education at the school.

A Disposal Log (Appendix H) will be maintained to list which records have been deleted, the date and description.

Personal details of pupil applicants which did "not progress" will be disposed of after 1 year.

Staff records will be securely disposed of 6 years after a member of staff leaves the employment of the school. Brief details will be retained on all staff indefinitely to satisfy future reference requests. These details will include full name, date of birth, job title, national insurance number and period of employment. Exceptions to this include records where there may be ongoing litigation in which case the entire record will be retained until final disposition of the matter and thereafter for a period of 6 years.

Unsuccessful staff applications should be kept for 6 months after interview.

Accident books / logs relating to all accidents in school should be kept for 40 years after the accident has been recorded as a claim could be made up to that time. The accident book must meet HSE accident book requirements.

An Accident: is any unplanned or undesired event that results in injury to a person which requires significant first aid intervention.

A flagging process should also be maintained to identify those records which should not be deleted due to litigation or other reasons. The flagging process and accident log should be referred to prior to records being deleted to identify any exceptions.

## 14. Subject access requests and other rights of individuals

### 14.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. 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

Subject access requests must be submitted in writing, either by letter, email or fax to the DPO. Written requests must include:

- Name of individual

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

Two forms of identification are required for the request to be processed.

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

If a parent makes a verbal subject access request to a member of staff, the member of staff must direct them to the office to make their request.

## **14.2 Children and subject access requests**

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

## **14.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- May contact the individual to clarify the information requested
- Will respond without delay and within 1 month of receipt of the request
- 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 this within 1 month, and explain why the extension is necessary

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

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.

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

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

## **14.4 Other data protection rights of the individual**

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 6), individuals also have the right to:

- Withdraw their consent to processing at any time (in certain circumstances)
- 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 of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

### **14.5 Exemptions to Access by Data Subjects**

Confidential references given, or to be given by the schools, are exempt from access. The schools will therefore treat as exempt any reference given by them for the purpose of the education, training or employment, or prospective education, training or employment of any pupil or member of staff.

It should be noted that confidential references received from other parties may also be exempt from disclosure. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

An exemption may also be considered in cases where a third party is identified and disclosure may be detrimental to that party

Data covered by Legal Privilege is also exempt i.e. where it may be necessary to take legal advice regarding a Data Subject; this information is exempt from Subject Access Request.

## **15. Parental requests to see the educational record**

Parents, or those with parental responsibility, have a legal right to 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. Training**

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

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

### **17. Monitoring arrangements**

The Headteacher/Business Manager is responsible for monitoring and reviewing this policy.

The DPO and DPC, checks that the school complies with this policy by, among other things, reviewing school records annually.

This document will be reviewed **every 2 years**.

At every review, the policy will be shared with the governing body.

## Appendix A: Definitions

Term	Definition
Personal data	<p>Any information relating to an identified, or identifiable, individual. This may include the individual's:</p> <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
Sensitive personal data	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> <li>• Whether a person has committed, or is alleged to have committed, an offence</li> </ul>
Processing	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
Data subject	<p>The identified or identifiable individual whose personal data is held or processed.</p>
Data controller	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
Data processor	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>

Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
----------------------	---

## **Appendix B: Roles and Responsibilities**

### **Role of the Data Protection Officer**

The role of the Data Protection Officer is to:

- Ensure that the organisation complies with the Data Protection Act and GDPR 2018, and to ensure that employees are fully informed of their own responsibilities for acting within the law and that the public, including employees, are informed of their rights under the Act.
- Be the nominated officer in the Data Protection register maintained by the Information Commissioner, notify the fact of processing to the Information Commissioner and maintain the accuracy and currency of the organisation's notification
- Co-ordinate Data Protection Act activities (including training) and facilitate such user group meetings as necessary e.g. Data Protection Coordinator's group
- Ensure organisational compliance, and conformance with the Data Protection Principles
- Develop, implement and enforce a suitable and relevant Data Protection policy and ensure it is reviewed on an annual basis
- To undertake systematic Data Protection Act compliance audits in accordance with Information Commissioner's audit tool
- Assist with investigations into complaints about breaches of the Act and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.
- Maintain a log of and co-ordinate Subject access requests.
- Maintain and update own knowledge of developments in Data Protection issues.
- Be a resource for other employees by providing expert advice on the Data Protection Act and related issues.

### **Role of the Headteacher**

- The Headteacher is responsible for the successful implementation of this policy in their school.
- The Headteacher will agree and authorise all data to be released in connection with a S.A.R. (Subject Access Request)

### **Role of the Data Protection Co-ordinator**

The role of the Data Protection Coordinator is to:

- Assist the Data Protection Officer to ensure compliance with this policy.
- This role will normally be carried out by J Handley & C Ashton.
- The Data Protection Officer will co-ordinate the compliance with the Data Protection Act and will be supported by the Data Protection Coordinator with the following:
  - On Site Data Security
  - Compliance Audit
  - Training
  - Subject Access Requests
  - Policy review
  - Housekeeping/Compliance e.g. data archiving, deletion etc.
  - CCTV compliance
  - Providing advice locally on aspects of DP compliance.

## Appendix C: Data Administrator Confidentiality Agreement

### Data Administrator Confidentiality Agreement

The school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore it is a data controller. Personal data can be processed in a paper format or an electronic format.

Your job role requires you to have access to the Data Systems we have in place to process personal data. When accessing and managing personal data you must at all times comply with the GDPR and DPA 2018. Use of the data must be consistent with the purpose for which the system was constructed. Data must be processed securely and not be subject to any unauthorised use or disclosure.

Staff who have the responsibility to access, add, amend and delete personal data must adhere to and comply with the following conditions:

The data is to be used only for educational purposes and in the interests of the person to whom that data belongs, and not for any other purposes.

Personal data is to be shared only with those who need the information to carry out an education function.

Only authorised staff may access, add, amend and delete personal data on the data systems and they must never share their login details with anyone.

Access to usernames and passwords is the responsibility of the nominated contacts in school who have a USO-OTP (One Time Password) Second Factor Authentication Device. Where necessary this responsibility may be shared with the system supplier (LGfL) and the system support supplier (WiBird)

Paper-based records that contain personal data must be 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

Personal data that is no longer needed must be disposed of securely. Personal data that has become inaccurate or out of date must also be disposed of securely. This includes shredding paper-based records and overwriting or deleting electronic files.

Procedures should be in place to protect any data in transit. If data needs to be taken out of the system it must be in an encrypted form.

Any breaches of data must be reported to the Data Protection Officer

Name:	
Role:	
Signature:	
Date:	

# Appendix D: Data Collection Sheet

## Data Collection Sheet

Please check that the information below is correct. Complete any missing details, and return to the school office.

<b>Surname:</b>	<b>Legal Surname:</b>
<b>Forename:</b>	<b>Middle name:</b>
<b>Chosen name:</b>	<b>Gender:</b>
<b>Date of Birth:</b>	<b>Year:</b>
<b>Address:</b>	<b>Reg Group:</b>
<b>Post Code:</b>	
<b>Telephone:</b>	
<b>Email:</b>	

Please give details of all persons who have parental responsibility and anyone else you wish to be contacted in an emergency. Place them in the order that you wish for them to be contacted in an emergency.

Priority	Name/Relationship	Home Address/Phone/Mobile/Fax	Work Address Phone/Email
1		Tel: Mobile:	Tel: Email:
2		Tel: Mobile:	Tel: Email:
3		Tel: Mobile:	Tel: Email:

<b>Dietary Needs</b>	
----------------------	--

<b>Medical Practice</b>	<b>Address</b>	<b>Telephone Number</b>
-------------------------	----------------	-------------------------

<b>Medical Condition(s)</b>
-----------------------------

<b>Medical Note(s)</b>
------------------------

<b>Ethnicity:</b>	<b>Religion:</b>
<b>Home Language:</b>	<b>First Language:</b>
<b>Country of Birth:</b>	<b>Nationality:</b>

The data being collected, controlled and processed is in line with General Data Protection Regulations (GDPR)

The school has a duty to protect this data and to keep it up to date. The school is required to share some of the data with the Education Authority and with the Department of Education

<b>Signature:</b>	<b>Date:</b>
-------------------	--------------



## Appendix E: Photo Consent form

### Photographs Consent

At Stanburn, we sometimes take photographs of pupils. We use these on the school's website, on dB Primary, in the school newsletter, for media coverage and on display boards around the school.

**If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption. If we name a pupil in the text, we will not use an individual photograph of that child to accompany the article. If a child has won an award and the parent would like the name of their child to accompany their picture, we will obtain permission from the parent before using the image.**

We would like your consent to take photos of your child, and use them in the ways described above. If you're not happy for us to do this, that's no problem – we will accommodate your preferences. Please complete the form below and return it to the school.

If you change your mind at any time, you can let us know by emailing the school office or just popping in to the school office to fill out a new form.

If you have any other questions, please get in touch.

Child's Name		Class	
I give permission for my child's image to be taken and used in school for displays and publicity material including printed and electronic publications, video and webcam recordings and on websites (eg school newsletter and school website)			Please tick
I do not want my child's image used for the school newsletter and website			

I have read and understood the conditions of use on the back of this form.

Parent/guardian signature: \_\_\_\_\_ Date: \_\_\_\_\_

Name: \_\_\_\_\_ Relationship to child: \_\_\_\_\_

#### Conditions of use

- This form is valid indefinitely from the date you sign it.
- We will not re-use any photographs or recordings a year after your child leaves this school. Historic photographs will remain on our school website.
- We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image or video, on our website, in our school prospectus or in any of our other printed publications.
- If we use photographs of individual pupils, we will not use the name of that child in the accompanying text or photo caption.
- If we name a pupil in the text, we will not use an individual photograph of that child to accompany the article.
- We may include pictures of pupils and teachers that have been drawn by the pupils.
- We may use group or class photographs or footage with very general labels, such as 'a science lesson' or 'sporting events.'
- We will only use images of pupils who are suitably dressed, to reduce the risk of such images being used inappropriately.
- Websites and social media platforms can be viewed throughout the world and not just in the United Kingdom where UK law applies.

## Appendix F: S.A.R. Request Form

### Subject Access Request

Article 15 of the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) grants you the right to access your personal data, if any, held by Stanburn Primary School.

Please complete this form if you wish to make a request in relation to your personal data.

**NOTE:** This is not a mandatory form – Subject Access Requests made in other formats will also be accepted but this form is designed to help you in providing us with the information we need to deal with your request and speed up the process.

### *Subject Access Request Guidance*

(Please read before filling in the Subject Access Request Form)

#### Which sections should I complete?

Sections 1, 2, 3 and 4	<b>Data Subject Details</b> Should be completed for ALL applications.
Sections 5, 6 and 7	<b>Representative Details and Authority to Release Information to a Representative:</b> Should only be completed if the application is being made by a representative (i.e. someone other than the data subject themselves).
Sections 2	<b>Proof of the applicant's identity:</b> If you do not have any of the forms of identity listed, we may in exceptional circumstances accept alternatives for consideration. (Current employees and pupils, you may visit the school office to confirm verification of your identity by an authorised member of staff).
Sections 6	<b>Proof of the representative's identity:</b> If you do not have any of the forms of identity listed, we may in exceptional circumstances accept alternatives for consideration.

## General Information

### How long will it take to get my data?

Once we are satisfied that you meet the criteria for disclosure of data under the General Data Protection Regulation, and have provided sufficient information for us to confirm your identity and accept your application for processing, you should receive a response within one calendar month from that date.

However, in certain circumstances, the GDPR allows us to extend that deadline depending on the complexity of your request. We will advise you within one month if we need to extend the response deadline.

Records may be held in several different locations in paper and electronic formats. If you only require specific information and you clearly state what that is – for example a specific document or IT-only data – then you are likely to get a quicker response.

### Cost

In most cases we will not charge a fee to comply with a Subject Access Request.

However, where the request is manifestly unfounded or excessive we may charge a “reasonable fee” for the administrative costs of complying with the request.

### Sending your completed form

Please send your completed form and proof of ID to:

Data Protection Officer  
Stanburn Primary School  
Abercorn Road  
Stanmore  
Middlesex HA7 2PJ

Or email FAO: Data Protection Officer at [office@stanburn.harrow.sch.uk](mailto:office@stanburn.harrow.sch.uk)

### Section 1 – Data Subject’s Details

Please provide the information in the space provided below.

We will only use the information you provide on this form to identify you and the personal data you are requesting access to, and to respond to your request.

<b>Title (please tick)</b>	<b>Mr</b> <input type="checkbox"/> <b>Mrs</b> <input type="checkbox"/> <b>Miss</b> <input type="checkbox"/> <b>Ms</b> <input type="checkbox"/> <b>Other</b> <input type="checkbox"/>
Surname	
First name(s)	
Date of birth	
Address	
Address	
City / County	
Postcode	
Telephone (daytime)	
Email address	
Relationship to the School	Employee <input type="checkbox"/> Pupil <input type="checkbox"/> Supplier <input type="checkbox"/> Other <input type="checkbox"/>

### Section 2 - Requests Proof of Data Subject's Identity

We will require proof of your identity before we can respond to your request.

In order to prove the applicant’s identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

**Please DO NOT send an original passport, driving licence or identity card**

List A ( <u>photocopy</u> of one from below)	List B ( <u>photocopy</u> of one from below)
Identification that clearly shows your name and date of birth.	Documentation that clearly shows your name and current address.
Passport/Travel Document	A Council Tax bill
Photo driving licence	Utility bill showing current home address
Foreign National Identity Card	Bank Statement or Building Society Book

**We reserve the right to refuse to act on your request if we are unable to identify you.**

If you do not have any of these forms of identification available, please contact our DPO for advice on other acceptable forms of identification: office@stanburn.harrow.sch.uk. Or if you are currently an employee or pupil at Stanburn Primary, you may visit the school office to confirm verification of your identity by an authorised member of staff.

**Section 3 – Information Requested**

So that we can locate the data you require efficiently, please answer the following questions to the best of your knowledge. Please continue on a separate sheet if necessary.

The Information Commissioner has stated that as much information as possible should be provided to assist with tracing a data subject’s information.

*Please tell us as much as you can about the information you are requesting about.*  
*For example, if you are requesting access to your personal data which might be in an email or document, it helps in our search to know who might have written it, when and to whom the information might have been sent, and where it may be stored.*

*Period attended/worked at **Stanburn Primary School**:*

*From \_\_\_\_\_ To \_\_\_\_\_*

*Specific period, which you request access to the data (complete if different from the period of attendance):*

*From \_\_\_\_\_ To \_\_\_\_\_*

---

**Section 4 - Declaration**

This form must be signed by you (the data subject).

*I request a copy of the relevant personal data that are held by **Stanburn Primary School** relating to information provided above. I confirm the information supplied is correct and I declare that I am the individual as indicated above.*

Signed \_\_\_\_\_ Date \_\_\_\_\_

## Section 5 - Requests Made on the Data Subject's Behalf

Please complete this section of the form with your name and contact details if you are acting on the data subject's behalf.

<b>First and last name</b>	
<b>Company name</b>	
<b>Address and Postcode</b>	
<b>Date of birth</b>	
<b>Telephone number</b>	

## ***Section 6 - Proof of the Representatives Identity***

We require proof of your identity before we can respond to your access request.

In order to prove the representative's identity, we need to see copies of two pieces of identification, one from list A and one from list B below. Please indicate which ones you are supplying.

**Please DO NOT send an original passport, driving licence or identity card**

<b>List A (<u>photocopy</u> of one from below)</b>		<b>List B (<u>photocopy</u> of one from below)</b>	
Identification that clearly shows your name and date of birth.		Documentation that clearly shows your name and current address.	
Passport/Travel Document		A Council Tax bill	
Photo driving licence		Utility bill showing current home address	
Foreign National Identity Card		Bank Statement or Building Society Book	

**We reserve the right to refuse to act on your request if we are unable to identify you.**

If you do not have any of these forms of identification available, please contact our DPO for advice on other acceptable forms of identification: [office@stanburn.harrow.sch.uk](mailto:office@stanburn.harrow.sch.uk).

**Section 7 - Authority to release information to a Representative**

A representative needs to obtain authority from the applicant before personal data can be released. The representative should obtain the applicant's signature below, or provide a separate note of authority. This must be an original signature, not a photocopy.

I hereby give my authority for the representative named in Section 6 of this form to make a Subject Access Request on my behalf.	
Signature of Applicant:	Date:
Signature of Representative:	Date:

**For office use**

Data Access Request Number	
Date request received	

## **Appendix G: S.A.R Release Letter**

[Name]  
[Address]

[Date]

Dear [Name of data subject]

### **Data Protection Act 2018: Subject Access Request**

Thank you for your correspondence of [date] making a data subject access request for [subject].

We are pleased to enclose the information you requested.

We have endeavoured to provide all the information that we hold on the data subject. However, if you have any reason to believe that there is any missing data then please do not hesitate to seek further clarity from us on this matter.

Yours Sincerely



## Appendix H: Disposal Log

### Stanburn: GDPR Data Disposal Annual Audit Log

Once per year the person responsible for a particular data set must date and initial to show that data has been disposed of in accordance with the schools data retention policy

School Year	Disposal of financial records over x years of age	Disposal of safeguarding records over x years of age	Disposal of SEN records over as per disposal dates indicated on files	Disposal of HR records over 6 years of age	Disposal of Contact information for pupils no longer at the school	Disposal of pupil record (paper and digital) over 7 years of age	Sample text	Sample text
2019/2020	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2020/2021	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2021/2022	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2022/2023	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2023/2024	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2024/2025	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2025/2026	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2026/2027	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2027/2028	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2028/2029	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2029/2030	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2030/2031	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2031/2032	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2032/2033	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2033/2034	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL
2034/2035	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL	DATE / INITIAL

## Appendix I: Privacy Notice (Parents and Pupils)

# PRIVACY NOTICE 2018 (Pupils & parents)

On 25 May 2018 the **European General Data Protection Regulation (GDPR)** replaces the Data Protection Act 1998.

## How we use pupil and parent information

Under General Data Protection Regulations (GDPR) we are obliged to inform you of the information we hold on and your child(ren), what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If it, or any information linked to is unclear, please contact the school office, or the school's Data Controller. Contact details for are available at the end of this privacy notice.

We, Stanburn Primary School, at Abercorn Road, Stanmore, HA7 2PJ are the Data Controller for the purposes of data protection law.

As a public body we have appointed a Data Protection Officer (DPO)

## 1. The categories of pupil & parent information that we collect, hold and share include but are not limited to:

- Personal information (such as name, unique pupil number and address, parents national insurance number).
- Contact details and preference (contact telephone numbers, email addresses, addresses)
- Characteristics (such as ethnicity, religion, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as data scores, tracking, and internal and external testing)
- Relevant medical information (such as NHS information, health checks, physical and mental health care, immunisation program and allergies)
- Special educational needs information (such as EHCP's, applications for support, care or support plans)
- Safeguarding information
- Exclusion information
- Behavioural information
- Photographs (for internal safeguarding & security purposes, school newsletters, media and promotional purposes).
- CCTV images
- Payment details

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

## 2. Why we collect and use this information

We use the pupil and parent data:

- to monitor and report on pupil progress
- to provide appropriate pastoral and medical care

- for safeguarding and pupil welfare purposes
- administer admissions waiting lists
- for research purposes
- to inform you about events and other things happening in the school
- to assess the quality of our services
- to comply with the law regarding data sharing

### 3. The lawful basis on which we use this information

Our lawful basis for collecting and processing pupil information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- (a) Data subject gives consent for one or more specific purposes.
- (c) Processing is necessary to comply with the legal obligations of the controller.
- (d) Processing is necessary to protect the vital interests of the data subject.
- (e) Processing is necessary for tasks in the public interest or exercise of authority vested in the controller (the provision of education).

Our lawful basis for collecting and processing pupil information is also further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special, information and the following sub-paragraphs in the GDPR apply:

- (a) The data subject has given explicit consent.
- (b) It is necessary to fulfil the obligations of controller or of data subject.
- (c) It is necessary to protect the vital interests of the data subject.
- (d) Processing is carried out by a foundation or not-for-profit organisation (includes religious, political or philosophical organisations and trade unions)
- (g) Reasons of public interest in the area of public health
- (i) It is in the public interest

A full breakdown of the information we collect on pupils can be requested from the school office.

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

An example of how we use the information you provide is:

*The submission of the school census returns, including a set of named pupil records, is a statutory requirement on schools under Section 537A of the Education Act 1996.*

*Putting the school census on a statutory basis:*

- *means that schools do not need to obtain parental or pupil consent to the provision of information*
- *ensures schools are protected from any legal challenge that they are breaching a duty of confidence to pupils*
- *helps to ensure that returns are completed by schools*

### 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 General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

## 5. Storing pupil data

We hold pupil data whilst the child remains at Stanburn Primary School. The file will follow the pupil when he / she leaves Stanburn Primary School. However where there is a legal obligation to retain the information beyond that period, it will be retained in line with our retention policy.

We have data protection policies and procedures in place, including strong organisational and technical measures, which are regularly reviewed.

## 6. Who we share pupil information with

We routinely share pupil information with appropriate third parties, including:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Schools that the pupils attend after leaving us

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

## 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 Department for Education (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 Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

## 8. Data collection requirements:

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

## 9. The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education 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 department 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 Department 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 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 department'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 department 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>

## **10. Requesting access to your personal data and your Data Protection Rights**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold, through a Subject Access Request.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with

- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer.

Parents/carers also have a legal right to access to their child's educational record. To request access, please contact [office@stanburn.harrow.sch.uk](mailto:office@stanburn.harrow.sch.uk) for attention of Mrs C Lansdown, Head.

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

## 11. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## 12. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data processor at [office@stanburn.harrow.sch.uk](mailto:office@stanburn.harrow.sch.uk).

## **Appendix J: Privacy Notice - Staff**

Under UK General Data Protection Regulations (UK GDPR) we are obliged to inform you of the information we hold on you, what we use it for, who we share it with, and for how long we keep it. This privacy notice (also known as a fair processing notice) aims to provide you with this information. If it, or any information linked to it is unclear, please contact the school office, or the school's Data Controller. Contact details for are available at the end of this privacy notice. We, Stanburn Primary School, at Abercorn Road, Stanmore, HA7 2PJ are the Data Controller for the purposes of data protection law.

This document is for all those employed to teach, or otherwise engaged to work, at the school to explain how personal information is used.

### **1. The categories of school information that we process**

These include:

- Contact details
  - Date of birth, marital status and gender
  - Next of kin and emergency contact numbers
  - Other personal information (such as name, employee or teacher number)
  - Other characteristics information (such as age, ethnic group)
  - Salary, annual leave, pension and benefits info
  - Bank account details, payroll records, national insurance number and tax status information
  - Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
  - Contract information (such as start date, hours worked, post, roles and salary information)
  - Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships (and, where relevant, subjects taught)
  - Performance information
  - Outcomes of any disciplinary and/or grievance procedures
  - Work absence information (such as number of absences and reasons)
  - Copy of driving licence
  - Photographs
  - CCTV footage
- 
- Data about your use of the school's information and communication system

- We may also collect, store and use information about you that falls into the ‘special categories’ of more sensitive personal data. This includes information about (where applicable):
  - Race, ethnicity, religious beliefs, sexual orientation and political opinions
  - Trade union membership
  - Health, including any medical conditions, and sickness records

The processing of this information is prohibited (GDPR – Article 9) unless certain conditions are met. See – Our lawful basis for holding this data.

## 2. Why we collect and use workforce information

We use workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- enable individuals to be paid
- inform the development of recruitment and retention policies
- facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- support effective performance management
- allow better financial modelling and planning
- enable ethnicity and disability monitoring
- improve the management of workforce data across the sector
- support the work of the School Teachers’ Review Body

## 3. Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Our lawful basis for collecting and processing staff information is defined under Article 6, and the following sub-paragraphs in the GDPR apply:

- to fulfil a contract we have entered into with you
- to comply with a legal obligation
- to carry out a task in the public interest
- in order to protect your vital interests (or someone else’s interests)

Less commonly, we may also use personal information, linked to special categories. Our lawful basis for collecting and processing this information is further defined under Article 9, in that some of the information we process is deemed to be sensitive, or special information and the following sub-paragraphs in the GDPR apply:

- you have given us explicit consent to use it in a certain way
- we need to protect your vital interests (or someone else’s interests)
- We have legitimate interests in processing the data – for example, where you have provided us with the consent to use your data, you may withdraw this consent at any time

We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school’s use of your data.



## 4. Collecting workforce information

We collect personal information via staff application and contract forms.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this and we will tell you what you need to do if you do not want to share this information with us.

## 5. Storing workforce information

We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment. You are able to have access to your file at any time to ensure that all information about you is up to date.

We hold data securely for the set amount of time shown in our data retention schedule. Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our retention schedule which currently states we will keep the information for six years for reasons such as: fulfilling a reference request.

<b>What we store</b>	<b>How/Where it is Stored</b>
Personnel files	Hard copies are kept securely in a locked cupboard in the HR officer's room. You can request to see your personnel files at any time through the Headteacher or HR Officer.
Appraisal documentation	Electronically on the leadership drive. Hard copies are kept in the HR officer's room. You can request to see your personnel files at any time through the headteacher.
Attendance information	Electronically in the School Information Management System (SIMS) and Dataplan's the School's external contractor payroll system. Hard copies are kept securely in a locked cupboard in the HR's officer's room. You can request to see your personnel files at any time through the Headteacher or HR Officer.

## 6. Who we share workforce information with

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals
- The Department for Education- to meet our legal obligations to share information linked to performance data.
- Your family or representatives- to carry out our public task in the event of an emergency
- Other staff members- to carry out our public tasks, for example having access to your school email address so that information can be shared effectively
- Our regulator Ofsted, in order to comply with our public task
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Central and local government to complete the legal obligation for things such as the workforce census
- Auditors- coming under a legal obligation, Harrow may be asked from auditors about financial information related to schools.
- Survey and research organisations- to meet our legal obligation in relation to ‘freedom of information’ requests
- Trade unions and associations- to carry out our public task in light of any key discussions within school linked to disciplinary/capability procedures or for events such as redundancy
- Security organisations- in order to keep our school secure and under the lawful basis of public task, we pass on certain staff member information so that they can be contacted if necessary (such as the caretaker)
- Health and social welfare organisations to carry out our public task in line with our attendance management policy with organisations such as occupational health
- Police forces, courts, tribunals- to meet our legal obligations to share certain information with it, such as safeguarding concerns or to carry out our public task in relation to a tribunal
- Employment and recruitment agencies- to meet the public task of supplying requested references.
- The governors- to carry out our public task within the school and remain accountable to them for finance and personnel issues
- Professional advisers and consultants – to enable them to carry out the service they have been contracted for
- Professional bodies

### Transferring data internationally

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

## 7. Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so. The Local Authority will use information about its school workforce for research and statistical purposes, and to evaluate and develop education policy and strategies. The statistics are used in such a way that individual staff cannot be identified from them. The LA may also use information to support and monitor schools regarding sickness and recruitment of staff.

### Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

## Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:

We are required to share information about our school employees with the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

## 8. Requesting access to your personal data

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 the Business Manager or the Headteacher.

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances. If you would like to make a request, please contact our data protection officer.

Depending on the lawful basis above, you may 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
- a right to seek redress, either through the ICO, or through the courts

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/>

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

## 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

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. To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

## 10. Contact

If you would like to discuss anything in this privacy notice, please contact the Business Manager or the Headteacher.

This notice is based on the Department for Education's model privacy notice for the school workforce.

## 11. How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

### ***Data collection requirements***

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

### ***Sharing by the Department***

The Department 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:

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

The Department 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 DfE releases personal 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 securely store and handle the data

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.

### **How to find out what personal information DfE hold about you**

Under the terms of the Data Protection Act 2018, you're entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the Department, you should make a 'subject access request'. Further information on how to do this can be found within the Department's personal information charter that is published at the address below:

<https://www.gov.uk/government/organisations/department-for-education/about/personal-information-charter>

To contact the department: <https://www.gov.uk/contact-dfe>