

# Data Protection Policy

2019 – 2020

Policy Updated: September 2019

Future Review: September 2020



# Nurture ~ Believe ~ Discover ~ Achieve

## OUR CHRISTIAN VISION

Our vision for Woodstock CE Primary School reflects a passionate commitment to learning and recognition of the uniqueness of individual learners. Guided by our Christian values, it is driven by our desire to offer the best possible education for our pupils in partnership with parents, the Church and the local community.

**Woodstock CE Primary School will be a centre for learning where adults and children:**

- ✓ **Nurture** and prioritise wellbeing and development.
- ✓ **Believe** in themselves and in each other.
- ✓ **Discover** their own strengths and become successful lifelong learners.
- ✓ **Achieve** more than they ever thought possible.

## OUR CHRISTIAN ETHOS

Recognising our historic foundation, we will preserve and develop our religious character in accordance with the principles of the Church of England and in partnership with the Churches at parish and diocesan level.

Woodstock CE Primary School strives to be an inclusive community where children grow, learn and achieve together. Within a nurturing, supportive and safe environment, mental health and wellbeing is at the heart of everything we do and recognised as the responsibility of all. Children's natural curiosity is fostered through a creative curriculum that excites and challenges, and enables them to be successful learners. Supported by a culture of equality and aspiration we aim to remove disadvantage so that every child can thrive.

We are committed to providing an education of the highest quality within the context of Christian belief and practice. We encourage an understanding of the meaning and significance of faith, and promote Christian values through the experience we offer to all our pupils.

*"For I know the plans I have for you", declares the Lord, "plans to prosper you and not to harm you, plans to give you hope and a future." Jeremiah 29, v11*



## Contents

1. Legal Framework
2. Aims
3. Legislation and guidance
4. The Data Controller
5. Roles and Responsibilities
6. Data protection principles
7. Collecting personal data
8. Subject access requests and other rights of individuals
9. Parental requests to see the educational record
10. Photographs and videos
11. Data protection by design and default
12. Data security and storage of records
13. Disposal of records
14. Personal data breaches
15. Training
16. Monitoring arrangements

Appendix One: Personal data breach procedure

Appendix Two: Privacy Notice – pupils

Appendix Three: Privacy Notice - school workforce

## Legal Framework

This policy has due regard to legislation, including, but not limited to the following:

- General Data Protection Regulation (GDPR 2018)
- Freedom of Information Act 2000
- Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998

This policy will be implemented in conjunction with the following other school policies:

- Acceptable User Policy (photography and videos)
- E-safety Policy
- Freedom of Information Policy
- Records Management Policy

## Aims

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 the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

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

## 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 personal information.](#)

[In addition, this policy complies with our funding agreement and articles of association](#)

## Definitions

Term	Definition
<p><b>Personal data</b></p>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>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>
<p><b>Special categories of personal data</b></p>	<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>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<p><b>Processing</b></p>	<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>
<p><b>Data subject</b></p>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<p><b>Data controller</b></p>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<p><b>Data processor</b></p>	<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>
<p><b>Personal data breach</b></p>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>

## 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.

## Roles and Responsibilities

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.

### Governing Body

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

### 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 Body with their advice and recommendations on school data protection issues.

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

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

Our DPO is Louise Askew and is contactable via Richard Graham, Business Manager.

### Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

### Business Manager

The Business Manager in liaison with the Headteacher and administrative team takes responsibility for the day-to-day processing of data.

### All staff

Staff 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 Business Manager, who in turn will contact 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 there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

## Data Protection Principles

The GDPR 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.

## Collecting Personal Data

### Lawfulness, fairness and transparency

We will only process personal data where we have one of six '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. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

### 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's records management policy.

## 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.

## Subject Access Requests and Other Rights of Individuals

### 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 or email to our Business Manager. They should include:

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

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

### **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 under 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 will 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.

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

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one 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.

## 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 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside 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.

## Parental requests to see the educational record

Parents, or those with parental responsibility have right of access to their child's educational record. This covers information such as the records of the pupil's academic achievements as well as correspondence from teachers, Local Authority employees and educational psychologists engaged by the school's Governing Body. It may also include information from the child and from you, as a parent. Information provided by the parent of another child would not form part of a child's educational record. The school will decide on a case-by-case basis whether to grant such requests, bearing in mind guidance issued from time-to-time from the Information Commissioner's Office.

The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

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

## Photographs and videos

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

We will obtain written consent from parents/carers, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent/carer. Uses may include:

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

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.

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 Child Protection Policy and our Acceptable User Policy for more information on our use of photographs and videos.

### **Data protection by design and default**

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).
- Completing 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).
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

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

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Acceptable Use Policy and Staff Handbook).
- 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).

### Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

### Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix One.

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

- A non-anonymised dataset being published on the school website which shows the test results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

### Training

All 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, guidance or the school's processes make it necessary.

### Monitoring Arrangements

The Business Manager in liaison with the Headteacher is responsible for monitoring and reviewing this policy. They in turn will ask the DPO to review and if appropriate revise the policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full Governing Body.

## Appendix 1: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO 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)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- 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:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO 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 on the school's computer system
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
  - 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
  - The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- 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
- If all the above details are not yet known, the DPO 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 DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO 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 DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - 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.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - 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 on the school's computer system

- The DPO and Headteacher will meet to 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.

*The following sets out examples of the relevant actions we will take for different types of risky or sensitive personal data processed by the school. For example:*

#### ***Sensitive information being disclosed via email (including safeguarding records)***

- *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.*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Services to recall it.*
- *In any cases where the recall is unsuccessful, the DPO 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.*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.*

- *The DPO 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.*

#### ***Sensitive information being disclosed on the school website***

- *If special category data (sensitive information) is accidentally made available on the website, the publisher must remove it as soon as they become aware of the error.*
- *Members of staff see the data must alert the publisher and the DPO as soon as they become aware of the error.*
- *If the publisher is not available or cannot remove it for any reason, the DPO will ask the IT Services to remove it.*

#### ***Non-anonymised pupil data or staff pay information being shared with governors***

- *If special category data (sensitive information) is accidentally made available via email to governors, the sender must attempt to recall the email as soon as they become aware of the error.*
- *Governors who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask IT Services to recall it.*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant governors 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.*
- *The DPO will ensure we receive a written response from all the governors who received the data, confirming that they have complied with this request.*
- *If special category data (sensitive information) is accidentally made available via paper to governors, the sender must request all governors return the information so that it can be shredded. The sender will ensure she/he receives a written response from all the governors who received the data, confirming that they have complied with this request.*

## Appendix 2: Privacy Notice (How we use pupil information)

### Why do we collect and use pupil information?

We collect and use pupil information under the General Data Protection Regulations 2018. Particularly under Article 6, where the information is collected and used because it is required by our school in order to carry out the task of educating and ensuring the welfare of our pupils.

We also collect and use pupil information in order to help pupils with additional special needs and requirements, so that we can ensure we offer the best possible support and resources to them (and their parents) during their time in our school.

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

- Personal information (such as name, unique pupil number and address; parental information; emergency contact information)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Medical information (such as name of GP, relevant medical conditions)
- Attendance information (such as sessions attended, number of absence, absence reasons)
- Behavioural information (such as behaviour incidents, exclusions)
- Assessment information (such as national curriculum assessments)
- Special educational needs information
- Safeguarding information
- School history (such as where pupils go when they leave us)
- Photographs
- Data about your use of the school's IT systems

### Why we collect and use this information

We use the pupil data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Assess the quality of our services
- Comply with the law regarding data sharing

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

We collect and use pupil information to meet legal requirements and legitimate interests set out in the Education Act 1996 and Regulation 5 of the Education Regulations 2013. To conform with GDPR, any information the school processes fulfils one of the following requirements from Article 6 of the GDPR:

- 1(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- 1(c) processing is necessary for compliance with a legal obligation to which the controller is subject.
- 1(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- 1(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Where we process special categories of personal data we do so under obligations covered in Article 9 of GDPR:

- 2(g) the processing is necessary for reasons of substantial public interest.



- Where the above do not apply the school will seek consent for specific purposes in line with the following Article 6.1.a.
- 1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

This will be done in writing and will clearly define any other uses of personal information and ask for consent for each and every use.

## 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.

## Storing Pupil Data

We hold pupil data for the time pupils are in school and beyond as appropriate (see Records Management Policy).

## With whom we share pupil information

We routinely share pupil information with:

- Schools that pupil's attend after leaving us
- Local Authority
- Department for Education (DfE)
- School Nurse

We also provide pupil level personal data to third party organisations which supply services to us for which the provision of the data is essential for the service to be provided. Decisions on whether to release this data are subject to a robust approval process, including the arrangements in place to store and handle the data. We currently provide pupil level data for the following purposes:

- Systems integral to the delivery of core business services, for example, Scomis, Capita, 123comms ParentMail
- Systems integral to the operation of IT Services systems, for example, Google, Lightspeed
- Curriculum products, for example, Mathletics, Spellodrome, Junior Librarian

A full current list is available on request.

## Photographs

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

We will obtain written consent from parents for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to the parent. Uses may include:

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

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.

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 Child Protection Policy and our Acceptable User Policy for more information on our use of photographs and videos.

## 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 and the DfE under Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

## 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>

## 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:

- Who is requesting the data
- Purpose for which it is required

- Level and sensitivity of data requested: and
- 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>

### 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, please contact our Business Manager, Richard Graham by email at [sbm@woodstock.oxon.sch.uk](mailto:sbm@woodstock.oxon.sch.uk) or by calling the school office on 01993 812209.

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.
- 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/>

### Contact

If you would like to discuss anything in this Privacy Notice, please contact:

Richard Graham  
Business Manager  
Woodstock CE Primary School  
Shipton Road  
Woodstock, Oxfordshire  
OX20 1LL  
Email: [sbm@woodstock.oxon.sch.uk](mailto:sbm@woodstock.oxon.sch.uk)  
Telephone: 01993 812209

## Appendix 3: Privacy Notice (How we use school workforce information)

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

- Personal information (such as name, employee or teacher number, national insurance number, address, phone number; next of kin and emergency contact numbers; and information to allow us to undertake our responsibilities in Disclosure and Barring Service checks)
- Special categories of data including characteristics information such as gender, age, race, ethnic group and, where relevant, medical information
- Contract information (such as start dates, hours worked, post, roles, salary, pension)
- Financial information (such as bank account details, tax status information)
- Recruitment information (such as proof of right to work in the UK, references, application form)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Performance information (such as appraisals, lesson observations, marking reviews, CPD records)
- Outcomes of formal procedures (such as disciplinary, grievance)
- Photographs
- Data about your use of the school's IT systems

### Why we collect and use this information

We use school workforce data to:

- enable individuals to be paid
- facilitate safe recruitment
- support effective performance management
- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- allow better financial modelling and planning
- enable ethnicity and disability monitoring

### The lawful basis on which we process this information

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

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

Where you have provided us with 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.

## Collecting this information

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.

## Storing this information

We create and maintain an employment file for each staff member. The information contained in the file is kept secure and is only used for purposes directly relevant to your employment. Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our Records Management Policy.

## Who we share this information with

We routinely share this information with:

- Our Local Authority
- Department for Education (DfE)
- Awarding bodies
- Ofsted

We also provide personal data to third party organisations which supply services to us for which the provision of the data is essential for the service to be provided. Decisions on whether to release this data are subject to a robust approval process, including the arrangements in place to store and handle the data. We currently provide school workforce data for the following purposes:

- Systems integral to the delivery of core business services, e.g. Scomis, Capita, 123comms (aka ParentMail)
- Systems integral to the operation of IT Services systems, e.g. Google, Microsoft, Lightspeed

A full current list is available on request.

## Why we share school workforce information

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

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.

We share personal data with the Department for Education on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

## Data collection requirements

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.

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>.

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.

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>

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

### 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 our Business Manager, Richard Graham [sbm@woodstock.oxon.sch.uk](mailto:sbm@woodstock.oxon.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 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/>

If you would like to discuss anything in this Privacy Notice, please contact:

Richard Graham  
Business Manager  
Woodstock CE Primary School  
Shipton Road  
Woodstock, Oxfordshire  
OX20 1LL  
Email: [sbm@woodstock.oxon.sch.uk](mailto:sbm@woodstock.oxon.sch.uk)  
Telephone: 01993 812209