# Data Protection Policy and Privacy Notices

<table>
<thead>
<tr>
<th>Reviewed:</th>
<th>Approved by the Resources Committee:</th>
<th>Date of next review:</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2018</td>
<td>8.5.18</td>
<td>Summer 2019</td>
</tr>
</tbody>
</table>
Contents

1. Aims ................................................................................................................................. 3
2. Legislation and guidance ................................................................................................. 3
3. Definitions .......................................................................................................................... 3
4. The data controller ........................................................................................................... 5
5. Roles and responsibilities ............................................................................................... 5
6. Data protection principles ............................................................................................... 6
7. Collecting personal data .................................................................................................. 6
8. Sharing personal data ....................................................................................................... 7
9. Subject access requests and other rights of individuals .................................................. 8
10. Parental requests to see the educational record ............................................................. 10
11. CCTV ............................................................................................................................... 10
12. Photographs and videos ................................................................................................ 10
13. Data protection by design and default ......................................................................... 11
14. Data security and storage of records ............................................................................ 12
15. Disposal of records ........................................................................................................ 12
16. Personal data breaches .................................................................................................. 12
17. Training .......................................................................................................................... 13
18. Monitoring arrangements ............................................................................................... 13
Appendix 1: Personal data breach procedure ................................................................. 14

Privacy notice - How we use pupil information? ............................................................ 17
Privacy notice - How we use school staff information? .................................................. 22
1. 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.

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. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data</td>
<td>Any information relating to an identified, or identifiable, individual. This may include the individual’s:</td>
</tr>
<tr>
<td></td>
<td>• Name (including initials)</td>
</tr>
<tr>
<td></td>
<td>• Identification number</td>
</tr>
<tr>
<td></td>
<td>• Location data</td>
</tr>
<tr>
<td></td>
<td>• Online identifier, such as a username</td>
</tr>
<tr>
<td></td>
<td>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</td>
</tr>
<tr>
<td>Special categories of personal data</td>
<td>Personal data which is more sensitive and so needs more protection, including information about an individual’s:</td>
</tr>
<tr>
<td><strong>Personal data</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Racial or ethnic origin</td>
<td></td>
</tr>
<tr>
<td>Political opinions</td>
<td></td>
</tr>
<tr>
<td>Religious or philosophical beliefs</td>
<td></td>
</tr>
<tr>
<td>Trade union membership</td>
<td></td>
</tr>
<tr>
<td>Genetics</td>
<td></td>
</tr>
<tr>
<td>Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</td>
<td></td>
</tr>
<tr>
<td>Health – physical or mental</td>
<td></td>
</tr>
<tr>
<td>Sex life or sexual orientation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Processing</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Data subject</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The identified or identifiable individual whose personal data is held or processed.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Data controller</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A person or organisation that determines the purposes and the means of processing of personal data.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Data processor</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Personal data breach</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</td>
<td></td>
</tr>
</tbody>
</table>
4. 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.

5. 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.

5.1 Governing body
The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 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 to the board 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 Karol Stelmaszczyk and is contactable via phone 0208 381 2188 or email office@woodlands.harrow.sch.uk.

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

5.4 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 DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
If they have any concerns that this policy is not being followed
If they are unsure whether or not they have a lawful basis to use personal data in a particular way
If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
If there has been a data breach
Whenever they are engaging in a new activity that may affect the privacy rights of individuals
If they need help with any contracts or sharing personal data with third parties

6. 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.

7. Collecting personal data
7.1 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.

7.2 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’s record retention schedule.

8. 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:
  o Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  o 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
  o 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 routinely share pupil information with:
• schools that the pupils attend after leaving us
• our local authority
• the Department for Education (DfE)
• our School Nursing Team.

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.

9. Subject access requests and other rights of individuals

9.1 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. 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 DPO.
9.2 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.

9.3 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
- 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.

9.4 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 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.

10. Parental requests to see the educational record
Parents, or those with parental responsibility, have a legal right to free access to their child’s educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

11. 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 Jyoti Radia, School Business Manager.

12. Photographs and videos
As part of our school activities, and for the purpose of assessing pupils we 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 their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don’t
need parental consent, we will clearly explain to the parent/carer and pupil how the photograph photograph and/or video will be used.

**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 and safeguarding, ICT and e-safety policies for more information on our use of photographs and videos.

### 13. 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;
- 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.

14. 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.
- Where personal information needs to be taken off site, staff must sign it in and out from the school office and use locked zip wallets.
- 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 e-safety policy, ICT policy, mobile phone policy and acceptable use agreement).
- 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).

15. 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.

16. 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 1.

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

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

17. 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.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this 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 board.
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’s 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.

**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 ICT department 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
Privacy notice - How we use pupil information?

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing ‘privacy notices’ (sometimes called ‘fair processing notices’) to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about pupils.

We, Woodlands School, are the ‘data controller’ for the purposes of data protection law.

Our data protection officer is Karol Stelmaszczyk, Assistant Headteacher (see ‘Contact us’ below).

The personal data we hold
Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Personal information such as contact details, contact preferences, date of birth, identification documents, unique pupil number
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, language, nationality, country of birth or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information such as sessions attendance, number of absences and absence reasons
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs and videos
- CCTV images captured in school

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

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
• Protect pupil welfare
• Assess the quality of our services
• Administer admissions waiting lists
• Carry out research
• Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils’ personal data when the law allows us to. Most commonly, we process it where:
• We need to comply with a legal obligation
• We need it to perform an official task in the public interest

Less commonly, we may also process pupils’ personal data in situations where:
• We have obtained consent to use it in a certain way
• We need to protect the individual’s vital interests (or someone else’s interests)

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.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily. Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our Record retention schedule, which is available on request, sets out how long we keep information about pupils.

Data sharing
We do not share information about pupils with any third party without 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 pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education on a statutory basis - this data sharing underpins school funding and educational attainment policy and monitoring.
- The pupil’s family and representatives
- Our regulator - Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Financial organisations
- Our auditors
- Survey and research organisations
- Health authorities
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals

**National Pupil Database**

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.

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](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](https://www.gov.uk/government/publications/national-pupil-database-requests-received)

To contact DfE: [https://www.gov.uk/contact-dfe](https://www.gov.uk/contact-dfe)

**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.

**Parents and pupils’ rights regarding personal data**

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your
personal information, or be given access to your child’s educational record, contact our school office.

You also have the right to:

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

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

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer: Karol Stelmaszczyk, office@woodlands.harrow.sch.uk, 0208 381 2188.
Privacy notice - How we use school staff information?

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing ‘privacy notices’ (sometimes called ‘fair processing notices’) to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, Woodlands School, are the ‘data controller’ for the purposes of data protection law.

Our data protection officer is Karol Stelmaszczyk (see ‘Contact us’ below).

The personal data we hold

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Personal information such as name, contact details, date of birth, marital status, employee or teacher number
- Special categories of data including characteristics information such as gender, age, ethnic group
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- 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
- Qualifications and employment records, including work history, job titles, contract information, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data
- Copy of driving licence
- Photographs
- CCTV footage
- Data about your use of the school’s information and communications system
We may also collect, store and use information about you that falls into "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

**Why we use this data**

The purpose of processing this data is to help us run the school, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- 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

**Our lawful basis for using this data**

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)
- We have legitimate interests in processing the data – for example, where:
  - [If you use this basis at all, set out the situations here]

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.

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.
**Collecting this information**

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us. Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

**How we store this data**

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.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule, which is available on request.

**Data sharing**

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 [maintained schools only] information about headteacher performance and staff dismissals
- The Department for Education
- Your family or representatives
- Our regulator - Ofsted
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll
- Financial organisations
- Our auditors
- Trade unions and associations
- Health authorities
- Health and social welfare organisations
- Professional advisers and consultants
- Police forces, courts, tribunals
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.

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 *data protection officer*.

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/

**Contact us**

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our *data protection officer*: Karol Stelmaszczyk, office@woodlands.harrow.sch.uk , 0208 381 2188.