

PRIVACY NOTICE

AUDIENCE: Parents, Carers, and Guardians

Introduction

Under data protection law, individuals have a right to be informed about how the Federation or school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

This privacy notice explains what rights you have with regards to your personal data and how you can exercise those rights.

This notice explains how we process personal data relating to parents, carers and guardians. Information about we process pupil data is provided separately in our Pupil Privacy Notice.

We, the White Horse Federation and school are the 'data controller' for the purposes of data protection law.

DPO Contact Details

If you need to contact us regarding your personal data, or if you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

Lyn Rouse – dpo@twhf.org.uk

The Personal Data We Hold

We process your personal data to fulfil our official functions, meet legal obligations, and support our interactions with you. This includes data collected at admission, throughout your time with our school(s), and in some cases after your child stops attending our schools.

The types of personal data we collect, process, store, and share include:

- Personal Identifiers
 - Full name
 - Home address(es)
 - National Insurance (NI) number
 - Date of birth
- Contact Information
 - Personal email addresses
 - Personal telephone numbers
 - Emergency contact details
 - Parental responsibility information

- Court orders
- Contact arrangements
- Collection permissions
- Financial Information
 - Bank account details (where supplied by you)
- Security and Monitoring Data
 - CCTV footage (for site security and safeguarding)
 - Phone call recordings (where applicable for training or safeguarding purposes)
 - Where parents access Trust provided systems, portals, guest Wi-Fi or online services
- Special Category Data (*processed under Article 9 UK GDPR*)
 - Ethnicity (for statutory reporting and inclusion)
 - Religion (for statutory reporting and inclusion)
 - Welfare factors (family medical or personal circumstances that might affect your or your child's emotional or physical wellbeing at school)

Why We Collect Your Personal Data

We collect and process your personal data to meet our legal and safeguarding obligations. Specifically, we use your data for the following purposes:

- **Communicate effectively with families**
Contact parents, carers, and guardians regarding pupil welfare, school updates, and emergencies.
- **Safeguard pupils and promote wellbeing**
Ensure the safety and welfare of pupils through appropriate pastoral care and safeguarding measures.
- **Support Student Welfare**
We may collect information about a parent or carer's health condition or personal circumstances where this helps us understand factors that may affect a pupil's wellbeing, attendance, behaviour, learning or access to education.
- **Manage admissions and transitions**
We use information and other details provided by parents and carers to administer admissions and support transition arrangements when pupils move between schools or educational phases.
- **Administer school trips and activities**
We collect your data so we can support the safe participation of pupils in school trips, activities and events.
- **Support families with additional needs**
Provide targeted assistance to families, including access to support services and funding.
- **Meet statutory reporting requirements**
Fulfil obligations to government bodies such as the Department for Education (DfE), Ofsted, and local authorities.

- **Manage school finances and funding**
Determine eligibility for financial support, such as free school meals and pupil premium. Your national insurance number is collected to assess and periodically review eligibility for FSM, PP and other funding support.
- **Comply with health and safety obligations**
Maintain records necessary for safeguarding, incident reporting, and emergency response.
- **Equality, Diversity, and Inclusion Monitoring**
To monitor and promote equality of opportunity and comply with public sector equality duties.
- **Crime Prevention and Security**
To support the detection and prevention of crime, including through CCTV, access control systems, and IT monitoring.
- **IT and System Access Management**
Where parents access Trust provided systems, portals, guest Wi-Fi or online services.

Lawful Basis for Processing Your Personal Data

We only collect and use personal data where we have a valid lawful basis under Article 6 of the UK General Data Protection Regulation (UK GDPR). The lawful basis we rely on will depend on the specific purpose of the processing. These are:

- **Public Task**
Most of our processing of parent and guardian information is necessary to enable us to carry out our educational, safeguarding and administrative functions and to maintain effective communication with families.
- **Legal Obligation**
We are required by law to collect and retain certain information, such as attendance records, safeguarding concerns, and data for statutory reporting to government bodies.
- **Vital Interests**
In exceptional circumstances, we may process personal data to protect someone's life, for example in a medical emergency.
- **Consent**
Where none of the other lawful bases apply, we may ask for your clear and informed consent to process specific types of data (e.g. use of photographs for promotional purposes). You have the right to withdraw your consent at any time by contacting the Data Protection Officer listed in this notice.
- **Legitimate Interests**
While public authorities cannot rely on this basis for processing related to their official tasks, we may use it for purposes outside our core public functions (such as parent engagement activities, school communications and community events). In such cases, we ensure that your rights and interests are not overridden and conduct a legitimate interests assessment.

Note:

We process special category data under, where applicable, and together with Schedule 1 conditions in the Data Protection Act 2018.

Article 9(2)(a) – Explicit consent,

Article 9(2)(c) – Vital interests,

Article 9(2)(f) – Legal claims, and

Article 9(2)(g) – Substantial public interest

Similarly, if we process *criminal offence data*, we meet the requirements of Article 10 and the Data Protection Act 2018.

How We Collect Your Personal Data

We collect personal data through various channels to comply with legal obligations. These include:

- **Directly from you** – for example, through admission forms, enrolment documents, and ongoing parent-school interactions.
- **From third parties** – where it is proportionate and lawful to do so, such as from:
 - Previous schools
 - Local authorities
 - Social care
 - Health services
 - Department for Education (DfE)
 - Admissions authorities

We may also collect data from internal systems (e.g. access logs, CCTV) and other sources where necessary and lawful.

Voluntary vs Mandatory Data

While much of the information we collect is required to meet our legal duties relating to education, safeguarding and administration, some information is provided on a voluntary basis. Where information is optional, we will make this clear at the point of collection. Examples may include parental surveys, feedback exercises, consent for the use of photographs or videos, participation in certain enrichment activities, or information provided to help us better understand and support a pupil's interests and wellbeing.

In other cases, providing personal data is **required by law or contract**. If you are required to provide specific data, we will explain:

- The legal basis for the requirement
- What may happen if the data is not provided (e.g. impact on admission eligibility or access to certain benefits)

We are committed to collecting only the data that is necessary for the stated purposes and ensuring that you are fully informed about how and why your data is used.

Where and How We Store Your Personal Data

We store your personal data securely in systems and locations appropriate to the type of information and its sensitivity. This includes both physical and digital storage solutions, which are protected by access controls and security protocols.

We maintain a file of parent details on Arbor MIS. This file is stored securely and accessed only by authorised personnel for legitimate purposes.

Digital data may be stored on secure servers, cloud-based platforms, or internal systems, all of which are subject to regular security reviews and data protection controls.

Sharing Your Personal Data

We do not share your personal data with third parties unless we have a lawful basis to do so.

This may include your consent, a legal obligation, or where it is necessary to perform our public duties and complies with data protection legislation.

Where sharing is required or permitted, we ensure that only the minimum necessary data is shared, and that appropriate technical and security safeguards are in place.

We may share your personal data with the following third parties, where it is lawful and proportionate to do so:

- **Family and Community**
 - Parents, carers, and legal representatives – to support pupil welfare and engagement
 - Parent-Teacher Collaboration – for school community activities and communications
- **Statutory and Regulatory Bodies**
 - Local authorities – to meet legal duties, including safeguarding concerns, exclusions, and education support purposes
 - Department for Education (DfE) – for statutory data collections and national education monitoring
 - Ofsted and other regulators – for inspection and compliance purposes
 - Central and local government – for policy, funding, and planning
- **Education and Assessment Partners**
 - Other schools or educational settings – during transitions or collaborative support
- **Health, Safety and Welfare Organisations**
 - Health authorities and school nurses – to support medical needs and public health initiatives
 - Social care and welfare services – where additional support or safeguarding is required
 - Security organisations – including for site safety and incident response
 - Police forces, courts, and tribunals – where required by law or for safeguarding purposes
- **Support and Advisory Services**
 - Professional advisers and consultants – for educational, legal, or operational support
 - Charities and voluntary organisations – where they provide direct support to pupils or families
 - Survey and research organisations – to help improve educational outcomes and services
- **Administrative and Technical Services**
 - Suppliers and third-party service providers – to deliver contracted services such as IT systems, catering, or transport
 - Financial organisations – for processing payments, funding, or financial support
 - Auditors – to ensure financial and operational accountability
- **Key Sub-processors** – we share personal data with third party edtech providers and technical solutions for many reasons, including to maintain operations, to monitor performance. These processors are analysed and evaluated to ensure compliance with data protection regulations. We identify some sub-processors as ‘key’ sub-processors,

whose functions are critical to operations and/or collect high levels of personal information.

Among others, our key sub-processors with whom your information may be shared include:

- **Arbor MIS** – Our core management information system for pupil, parent, and school staff information.
- **CPOMs** – Our safeguarding information management system.
- **OneTrust** – The platform used to process, action, and provide information requested in a Subject Access Request.
- **Microsoft 365**

We ensure that all third parties receiving personal data are subject to appropriate data protection obligations and contracts, and we do not allow them to use your data for their own purposes.

Transferring Data Internationally

We do not routinely transfer personal data outside the UK or European Economic Area (EEA). However, in specific circumstances — such as organising a residential trip abroad — we may need to share limited personal data with organisations or individuals based outside the EEA (e.g. accommodation providers, travel companies, or host schools).

Some of our service providers, including Microsoft, may process personal data outside the UK. Appropriate safeguards will be implemented, including adequacy regulations, international data transfer agreements, or another recognised UK GDPR transfer mechanism.

Your Right to Access Your Personal Data

Under UK data protection law, you have the right to request access to personal data that we hold about you. This is known as a **Subject Access Request (SAR)**, and it is one of your rights under the UK General Data Protection Regulation (UK GDPR).

If you submit a SAR, we will assess your request in accordance with data protection legislation.

As an individual you are entitled to:

- Confirmation that we are processing your personal data
- A description of the data we hold
- The purposes for which we are processing it
- How long we intend to retain it
- The source of the data, if not collected directly from you
- Details of any recipients or categories of recipients
- Information about any automated decision-making and its consequences
- A copy of the data in an accessible format

Please note that we may need to redact or withhold certain information where disclosure would adversely affect the rights or freedoms of others, or where exemptions apply under the Data Protection Act 2018.

You may also have the right to request that your personal data be transmitted electronically to another organisation, where technically feasible and lawful.

We aim to respond within **one calendar month** and will inform you if an extension is required due to the complexity of your request.

If you would like to make a request, please email DPO@twhf.org.uk or log a request through our website.

Your Other Rights Regarding Your Personal Data

Under UK data protection law, you have a number of rights concerning how your personal data is used and protected. These rights are not absolute and may be subject to conditions or exemptions, but we will always consider any request you make in line with the law.

You have the right to:

- **Object to processing** based on public task or legitimate interests in certain circumstances.
- **Object to direct marketing**, including profiling related to direct marketing.
- **Object to automated decision-making**, including profiling, where decisions are made solely by automated means and have legal or similarly significant effects.
- **Request rectification** of inaccurate or incomplete personal data.
- **Request erasure** of your personal data, also known as the “right to be forgotten,” in certain circumstances.
- **Request restriction** of processing, for example, while a dispute over accuracy or lawfulness is being resolved.
- **Request data portability**, allowing you to obtain and reuse your personal data across different services, where applicable. This right only applies where processing is based on consent or contract and carried out by automated means.
- **Claim compensation** for damages caused by a breach of data protection legislation, where applicable.

Use of Artificial Intelligence (AI)

The Trust uses approved AI technologies to help support teaching, learning and administrative activities. Any use of AI involving personal data is subject to appropriate data protection, security and safeguarding controls. AI may assist staff with certain tasks, but it does not replace professional judgement. Decisions about pupils and parents are not made solely by AI and always involve meaningful human oversight.

Data Retention

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, including to meet legal, regulatory, and operational requirements. After your time with us ends, your data will be retained and then securely deleted in accordance with our Retention Policy, which outlines specific retention periods for different categories of data.

Complaints

We take concerns about the handling of personal data seriously. If you believe that our collection or use of your personal information is unfair, misleading, inappropriate, or otherwise causes concern, we encourage you to raise this with us in the first instance. You can make a data protection complaint by contacting our Data Protection Officer.

DPO@twhf.org.uk

If you are not satisfied with our response, or believe that your data protection rights have been infringed, you have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent regulator for data protection:

Online: [Report a concern](#)

Phone: 0303 123 1113

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Version	Date of Change	Summary of Changes
V2	Aug 2025	Updates in line with 2025 regulations
V3	Aug 2026	Clarification on complaints information in line with DUAA, added key sub-processors. Updated AI section,