T: 01793 818603
www.twhf.org.uk

PRIVACY NOTICE

AUDIENCE: Employees, Contractual Staff and Other Workforce Members

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.

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 the effective management of your employment. This includes data collected at recruitment, throughout your employment, and in some cases after your employment ends.

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

1. Personal Identifiers
    - Full name
    - Home and work addresses
    - National Insurance (NI) number
    - Teacher reference number (where applicable)
    - Date of birth
    - Employee ID
    -
2. Contact Information
    - Personal and work email addresses
    - Personal and work telephone numbers
    - Emergency contact details

3. Employment and Professional Data
   - Job title and role
   - Employment history
   - Qualifications and training records
   - Performance appraisals
   - Grievance and disciplinary records
   - Absence and leave records (including sickness and parental leave)
   - Driving licence number (where relevant to role)
   -

4. Special Category Data *(processed under Article 9 UK GDPR)*
   - Ethnicity (for equal opportunities monitoring)
   - Health information (e.g. medical conditions, occupational health assessments)
   - Trade union membership (where declared)

5. Financial and Payroll Information
   - Bank account details
   - Salary and pension information
   - Tax and benefits data

6. Security and Monitoring Data
   - CCTV footage (for site security and safeguarding)
   - Photographs (for ID badges and internal systems)
   - Phone call recordings (where applicable for training or safeguarding purposes)
   - IT usage logs and access records

Why We Collect Your Personal Data
We collect and process your personal data to support the effective management of your employment and to meet our legal, contractual, and safeguarding obligations. Specifically, we use your data for the following purposes:

Human Resources Management
To administer employment relations, recruitment, onboarding, retention, and contract management.

Payroll and Pensions Administration
To ensure accurate payment of salaries, pension contributions, and statutory deductions.

Training, Development, and Support
To provide access to professional development opportunities, performance reviews, and wellbeing support.

Workforce Planning and Reporting
To build a comprehensive picture of the workforce, including deployment, diversity, and staffing needs.

Safer Recruitment and Safeguarding
To comply with statutory safeguarding requirements, including *Keeping Children Safe in Education (KCSIE)*, and to ensure suitability for roles involving children and vulnerable individuals.

Legal and Regulatory Compliance
To meet obligations under employment law, health and safety regulations, and data protection legislation.

Crime Prevention and Security
To support the detection and prevention of crime, including through CCTV, access control systems, and IT monitoring.

Legal Claims and Proceedings
To establish, exercise, or defend legal claims, including employment disputes and tribunal cases.

Health and Wellbeing Management
To assess and support employee health, including occupational health referrals and reasonable adjustments.

Equality, Diversity, and Inclusion Monitoring
To monitor and promote equality of opportunity and comply with public sector equality duties.

Communication and Engagement
To facilitate internal communications, staff surveys, and engagement initiatives.

IT and System Access Management
To manage access to digital systems, ensure cybersecurity, and monitor appropriate use of technology.

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 is necessary to perform a task carried out in the public interest or in the exercise of our official functions, such as delivering education and ensuring safeguarding. This basis has a clear foundation in law.

Legal Obligation
We process certain data to comply with legal requirements, such as employment law, health and safety regulations, and statutory record-keeping obligations. This does not include contractual obligations.

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 (e.g. internal communications or wellbeing initiatives). In such cases, we ensure that your rights and interests are not overridden and conduct a legitimate interest's assessment.

Note:
Where we process *special category data* (e.g. health, ethnicity, trade union membership), we also identify and document an additional lawful condition under Article 9 of the UK GDPR.

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 support employment-related processes and comply with legal obligations. These include:

- **Directly from you** – for example, through application forms, onboarding documents, and ongoing HR interactions.

- **From third parties** – such as:
  Disclosure and Barring Service (DBS) providers
  Previous employers (via references)
  Occupational health professionals
  Recruitment agencies (where applicable)

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

Voluntary vs Mandatory Data
In some cases, providing personal data is **optional**. Where this applies, we will clearly inform you and explain any consequences of not providing the data.
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 or contractual basis for the requirement
- What may happen if the data is not provided (e.g. impact on employment 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 an employment file for each staff member, which contains information relevant to your role and employment. 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 safeguards are in place.

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

Local Authorities – to meet statutory obligations, including safeguarding concerns and reporting on leadership performance or staff dismissals.

Department for Education (DfE) – for workforce census and statutory reporting.

Your Family or Representatives – in emergency situations or where you have provided consent.

Educators and Examining Bodies – for professional development, certification, or qualification purposes.

Regulators – such as Ofsted or the Independent Schools Inspectorate, for inspection and compliance purposes.

Suppliers and Service Providers – including payroll processors, HR systems, and IT support, to deliver contracted services.

Financial Organisations – for salary, pension, and benefits administration.

Central and Local Government – where required for policy, funding, or compliance purposes.

Auditors – for financial and operational audits.

Survey and Research Organisations – only with your explicit consent.

Trade Unions and Professional Associations – where applicable.

Health Authorities and Occupational Health Providers – for health assessments and support.

Security Organisations – for safeguarding and site security.

Social Welfare Organisations – where support or intervention is required.

Professional Advisers and Legal Consultants – for employment law advice or dispute resolution.

Charities and Voluntary Organisations – where relevant to staff wellbeing or support services.

Police, Courts, and Tribunals – where required for legal proceedings or investigations.

Disclosure and Barring Service (DBS) – for safeguarding checks.

Employment and Recruitment Agencies – where applicable to your role or contract.

Employers of Contractual Staff – for coordination and compliance with employment terms.

IT and Software Providers – including cloud-based platforms and internal systems used to store and manage staff data.

Legal Representatives and Insurers – where necessary for legal advice or insurance claims.

Training Providers – for delivery of CPD, safeguarding, or compliance training.

Professional Licensing or Accreditation Bodies – for roles requiring registration or certification.
Emergency Services – in urgent situations to protect life or safety.

Data Processors for Surveys or Analytics – where external platforms are used for staff surveys or workforce analytics.

Cloud Hosting and Data Backup Providers – where staff data is stored or backed up externally.

Internal Governance Bodies – such as Trust Boards or HR Committees, for oversight and decision-making.

Under Schedule 2, Part 3, Paragraph 17 of the Data Protection Act 2018, it is generally considered reasonable to disclose staff names when responding to Subject Access Requests (SARs) or when transferring safeguarding information.

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).
In such cases, we will:

- Only share the minimum necessary data required for the purpose.
- Obtain your **explicit consent** before any international transfer takes place.
- Ensure that appropriate safeguards are in place to protect your data, in line with UK data protection law.

Your Rights – Accessing 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 the processing of your personal data where it is likely to cause, or is causing, substantial damage or distress.

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.

Claim compensation for damages caused by a breach of data protection legislation, where applicable.

Use of Artificial Intelligence (AI)
We use artificial intelligence (AI) tools within the organisation to support certain administrative and operational processes, such as document management, data analysis, or communication support. However, we do **not** use AI to make decisions about individuals that have legal or similarly significant effects. If we decide to introduce AI for decision-making purposes in the future, we will inform you in advance and update this privacy notice accordingly.

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.
Once your employment 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 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

Last updated 15th August 2025
Version 3