Pinnacle Learning Trust Job Applicant Privacy Notice 25-26

This privacy notice describes how The Pinnacle Learning Trust ('the Trust') handles personal data you submit when applying for a job. Please read this document to ensure that you understand how your data will be processed and safeguarded.

The Pinnacle Learning Trust complies with the GDPR and is registered as a "Data Controller" with the Information Commissioner's Office (Reg. No. ZA341736). The Data Protection Officer (DPO) for the Trust is **Corinne Walker**. Contact details are at the end of this document. We ensure that applicants personal data is processed fairly and lawfully, is accurate, kept secure, retained for no longer than is necessary, and disposed of securely, in line with the Trust's Retention Policy.

Why do we need to process applicant personal data?

As part of the Trust's recruitment process, certain information needs to be collected so your application can be considered. The Trust has the legal right and a legitimate interest to collect and process personal data relating to its prospective employees to ensure that the Trust's safeguarding and safer recruitment policies are upheld. The Trust processes personal data to meet the requirements set out in UK employment and childcare law.

Providing your data is voluntary. However, if you decline to submit requested candidate data, our ability to consider you as a candidate may be limited. By submitting an application to the Trust, you are consenting to the processing of your data for the purpose of forming a contract should you be successful in your application.

If you are successful in your application, you will be provided with a separate privacy notice in relation to any further processing of your data prior to the commencement of your employment. If your application is unsuccessful, your data will be retained and/or destroyed in accordance with the Trust's data retention policy.

The lawful basis for processing personal data pertaining to prospective members of staff is for the purposes of forming a contract. The data will be used for the following reasons:

- To carry out pre-employment checks, e.g. right to work in the UK
- To comply with legal or regulatory requirements.
- To assess your skills, qualifications, and suitability for the work or role.
- To carry out an online search as part of our due diligence on all shortlisted candidates.
- To enable ethnicity and disability monitoring
- To allow better financial modelling and planning
- To inform the development of recruitment and retention policies
- To communicate with you about the recruitment process.

For all roles, the Trust is obliged to seek information about criminal convictions/offences. Where it seeks this information, it does so because it is necessary for it to carry out its obligations and exercise specific rights in relation to employment.

The Trust will not use your data for any purpose other than recruitment.

What information does the Trust collect?

It collects a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number;
- Details of your skills, experience and employment history, including absence;
- Education & qualifications including photographs and images from recorded assessments;
- Information about your current level of remuneration, including benefit entitlements;
- Whether or not you have a disability for which the Trust needs to make reasonable adjustments during the recruitment process;
- Nationality, visa, proof of right to work permit information including passport, driving licence, national insurance number;

- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health, and religion or belief;
- Social media handles
- Criminal convictions

The Trust collects this information in a variety of ways. For example, data might be contained in application forms, CVs or cover letters, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment. Recruitment agencies also regularly provide personal data, primarily in the form of candidate CVs.

Special categories of information

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations. The Trust processes health information if it needs to make reasonable adjustments to the recruitment process for candidates who have a disability. This is to carry out its obligations and exercise specific rights in relation to employment.

Where the Trust processes other special categories of personal data, such as information about ethnic origin, sexual orientation, religion or belief, this is done for the purposes of equal opportunities monitoring with the explicit consent of job applicants, which can be withdrawn at any time. This includes, but is not restricted to:

- Information about any medical conditions we need to be aware of, including physical and mental health
- racial or ethnic origin
- data concerning a person's sex life or sexual orientation
- political opinion
- trade union membership
- religious or philosophical beliefs
- Photographs and CCTV images captured in school
- Information about characteristics, such as ethnic background or special educational needs (SEN)
- Biometric data used to identify you (for example; fingerprint scanning for academy meals - Hathershaw only)

This information is used to ensure that we meet our obligations under the Equality Duty and also to ensure that we provide support to you throughout your time with us.

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and 1 of the following conditions for processing as set out in UK data protection law:

- We have obtained your explicit consent to use your personal data in a certain way
- We need to perform or exercise an obligation or right in relation to employment, social security or social protection law
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for the establishment, exercise or defence of legal claims
- We need to process it for reasons of substantial public interest as defined in legislation
- We need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional, or by any other person obliged to confidentiality under law
- We need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- We need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in UK data protection law. Conditions include:

- We have obtained your consent to use it in a specific way
- We need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent
- The data concerned has already been made manifestly public by you
- We need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- We need to process it for reasons of substantial public interest as defined in legislation

Who do we share your information with?

Your information will be shared internally for the purposes of the recruitment exercise. This includes members of the HR team, interviewers involved in the recruitment process, other recruitment decision-makers in the Trust and IT staff if access to the data is necessary for the performance of their roles.

The Trust will not share your data with third parties, unless your application for employment is successful and it makes you an offer of employment. The Trust will then share your data with former employers to obtain references for you, employment background check providers and (where required) regulatory bodies to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal records checks.

How does the Trust store and secure data?

Data is stored in a range of different places, including the applicant information management systems, on paper in stored secure places, or on electronic documents within a secure network, in HR management systems and on other IT systems (including email).

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality. There are procedures in place to deal with any suspected personal data breach and we will notify you and any applicable regulator of a breach where we are legally required to do so.

How long does the Trust keep personal information for?

Personal data is retained in accordance with the Trust's data retention policy and will be disposed of in accordance with that policy. If you require further information regarding retention of data and the periods for which your personal data is held for, please contact the DPO (see below).

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment. The periods for which your data will be held will be provided to you in a new privacy notice.

Filtering and monitoring

Whilst on the premises of an academy within the Trust, we may monitor your use of our information and communication systems, equipment and facilities (e.g. school computers). We do this so we can:

- Comply with health and safety, and other legal obligations
- Comply with our policies (e.g. child protection policy, IT acceptable use policy) and our legal obligations
- Keep our network(s) and devices safe from unauthorised access, and prevent malicious software from harming our network(s)
- provide a safe environment for children and young people

Inappropriate activity (even personal communication) will be reported to the DSL and/or Principal, which may result in disciplinary action.

CCTV

All Trust academies use CCTV systems to ensure the safety and security of all applicants, staff and visitors. All footage is stored for no longer than six weeks and is automatically overwritten, unless it is to be used in evidence for a criminal case. The CCTV cameras are sited to ensure that only public or common areas within the Trust sites are recorded. The cameras are positioned so that no members of the public are inadvertently recorded.

In addition, Oldham Sixth Form College operates a Body-Worn Camera system that can record audio and visual footage. All CCTV/BWC cameras are limited to use by authorised users only. All policies are available on the Trust website.

Photographs

The Academies within the Trust may take photographs, videos or webcam recordings for official use, marketing and for educational purposes. You will be made aware that this is happening and the context in which the photograph will be used. Photography and video content is kept indefinitely as it may have historical significance unless a participant requests that their personal data be deleted.

Transferring data internationally

The Trust will not transfer your data outside the European Economic Area.

Automated decision-making

Currently automated decision making is not used to make decisions on applications. If we ever propose to make decisions about you using only automated systems, we will explain this to you. Automated decisions are always subject to human involvement and overview. If this changes in the future, we will amend any relevant privacy notices to explain the processing to you, including your right to object to it.

Artificial Intelligence

Personal data may be contained within documents uploaded to our AI Tools. We are the data controller of your personal data when it is used, and the AI supplier/contractor is a data processor. We have a signed agreement in place with each supplier/contractor to ensure that your personal data is protected. Users of our AI Tools know how to process personal data in accordance with the UK GDPR and our data protection policies.

In most cases, we process your personal data using the AI Tools to improve the efficiency, quality, and speed of our processes. A lot of these processes are already happening manually. Using AI to automate these processes allows our resources to be used where they are needed most. Any AI tools a school chooses to employ (e.g., AI marking or assessing) would be explained to applicants and parents/carers and would always be subject to human oversight and human intelligence. Depending on which AI tool is used, consent from parents/carers may be required. Consent will be gained prior to purchase and use.

Any supplier who has access to your data is assessed for compliance with Data Protection legislation before any information is processed by them. None of your personal data is used solely by the AI technology provider to improve their AI products.

What are your rights?

Under data protection legislation, applicants have the right to request access to information about them that we hold. To make a request for your personal information, contact the Data Protection Officer (details are below)

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

Withdrawal of Consent

The lawful basis upon which the Trust processes personal data is that it is necessary in order to comply with the Trusts legal obligations and to enable it to perform tasks carried out in the public interest.

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 would go about withdrawing it.

Complaints

We take any complaints about our collection and use of personal information very seriously. If you have a concern that our collection or use of personal information is unfair, misleading, or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance. We will acknowledge complaints within 30 days and advise you of the outcome without undue delay. Our DPO (Data Protection Officer) is **Corinne Walker** and details of how to contact her are below. Alternatively, you can seek advice directly from the Information Commissioner's Office, the UK's data protection regulator: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Further Information

If you would like to discuss anything in this privacy notice, please contact: Corinne Walker, Data Protection Officer, The Pinnacle Learning Trust, C/o Oldham Sixth Form College, Union Street West, Oldham, OL8 1XU, Tel: 0161 287 8000 ext 2314

Email: dataprotection@pinnaclelearningtrust.org.uk

Changes to this privacy notice

We may change this privacy notice and we encourage you to check this privacy notice from time to time.