The Active Learning Trust
ACTIVE LEARNERS · ACTIVE LEADERS · ACTIVE CITIZENS

Job Applicants Privacy Notice

To be reviewed on an annual basis by the Trust Board

History of Document

Issue No	Author	Date Reviewed	Approved by Trust Board	Comments
1	DPO	13/11/18	-	1st issue
2	DPO	18/11/18	-	Add data controller, what is personal data & consequences of non provision, how long held and individuals rights
3	DPO	8/1/20	-	CCTV added
4	DPO	20/8/20	-	Covid-19 pandemic – track and trace
5	DPO	23/11/20	17/12/20	Data shared internationally, more information on an individual's rights and how to complain
6	DPO	May 2021	27/5/21	Social media reference – inclusion of personal social media
7	DPO	June 2022	14/7/22	Changes to Overview, lawful basis and data protection
8	DPO	6/3/23		Change of DPO and Data Controller address

Overview

Under data protection law, individuals have a right to be informed about how the Active Learning Trust ("Trust") uses personal data that it holds about them. The Trust complies with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where it processes their personal data.

The Trust is committed to protecting the privacy of the individuals whose data it processes and to undertaking all data processing in a lawful, open and transparent way.

As an employer, the Trust collects and processes a prospective employee's personal data for employment purposes. It will process a prospective employee's personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Should a job application be successful, when an individual starts to work for the Trust, another privacy notice will be provided that explains how the Trust processes an employee's personal data whilst working for the Trust.

Data Controller

The Active Learning Trust is the "Controller" for the purposes of data protection law. This means that it is responsible for deciding how it holds and uses personal data about job applicants. Its address is Cromwell Community College, Wenny Road, Chatteris, Cambridgeshire, PE16 6UU.

The Trust's Data Protection Officer is the ICT Service, email: dpo@theictservice.org.uk . As Data Protection Officer, they are responsible for informing and advising the Trust about its data protection law obligations and monitoring its compliance with these obligations. They also act as a job applicants' first point of contact if they have any questions or concerns about data protection.

What is Personal Data?

Personal data means any information relating to a living individual who can be identified (directly or indirectly) in particular by reference to an identifier (e.g. name, NI number, email address, physical features). It can be factual (e.g. contact details or date of birth), an opinion about an individual's actions or behaviour, or information that may otherwise impact that individual in a personal or business capacity.

Data protection law divides personal data into two categories: ordinary personal data and special category data. Any personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life or

sexual orientation, biometric or genetic data that is used to identify an individual is known as special category data. (The rest is ordinary personal data).

Categories of Personal Data that the Trust processes

The Trust processes personal data relating to those applying to work for the Trust. Personal data that it may collect, use, store and share (where appropriate) about a job applicant includes, but is not restricted to the following from a job applicant's application form, covering letter and references:

- Contact details (such as name, address, contact numbers, email address)
- Characteristics information (such as gender and age)
- Recruitment information (such as references and curriculum vitae)
- Evidence of qualifications
- National insurance number
- Employment records, including work history, job titles, current salary, reasons for wanting to leave, training records and professional memberships, experience and skills, teacher number
- Information about a job applicant's current level of remuneration, including benefit entitlements
- Criminal records, convictions, cautions, reprimands, final warnings, bans
- Images captured by CCTV at the school's premises and in any school - owned areas or mode~~s~~ of transport etc – if the school has CCTV and a job applicant visits the school or attends an interview.

Also

- Publicly available information about a job applicant, such as their business and personal social media presence
- Selection information, including correspondence, interview notes, internal notes, the results of any written or online selection tests

If a job applicant is shortlisted for a position, or they receive a conditional offer of employment, the Trust may collect, hold and use the following additional types of ordinary personal data about them:

- Pre-employment check information, including references and verification of qualifications
- Right to work checks and related documents

The Trust may also collect, use, store and use information about a job applicant that falls into special categories of more sensitive personal data. This may include:

- Characteristics information (such as race, ethnicity, religious beliefs, sexual orientation, religious belief and political opinions).
- Relevant medical information (such as disabilities, health, allergies and access requirements).

Additional information:

- A job applicant may be asked to email the Trust digital copies of their documentation, including identification documents, right to work documentation and qualifications. Any requested documentation should be password protected with the password sent separately or provided verbally by phone. The original documentation will be required to be presented in person in school as soon as it is possible to do so.

- Interviews may be conducted remotely, by telephone or online using Microsoft Teams or Zoom. Where practical, interviews may be recorded to facilitate the recruitment process.

Why the Trust collects Personal Data

The Trust processes such personal data to aid in the recruitment process to:

- Enable it to establish relevant experience and qualifications
- Facilitate safe recruitment as part of its safeguarding obligations towards pupils/students
- Identify a job applicant and safely evacuate the school in the event of an emergency
- Enable equalities monitoring
- Ensure that appropriate access arrangements can be provided for applicants that require them
- Enable the Trust to recruit

How the Trust collects Personal Data

When the Trust collects personal information on its forms, it will make it clear whether there is a lawful requirement for a job applicant to provide it, and whether there is a legal requirement on the school to collect it. If there is no legal requirement then the Trust will explain why it needs it and what the consequences are if it is not provided.

The Trust also collects information from previous employer(s) or educational establishment(s). A Job Applicant will know about this because they will have supplied the Trust with the relevant contact details.

Lawful Basis for collecting and processing Personal Data

The legal basis the Trust relies on for processing a job applicant's personal data are:

- To satisfy the Trust's legal obligations for example it is mandatory to check a successful applicant's eligibility to work in the UK before employment starts and to keep a record of the Trust's decision making and monitor and comply with its responsibilities under the Equality

Act 2010.

- Legitimate interest – the Trust has a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows the Trust to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job.

- Consent - A Job Applicant may have given the Trust consent to use their personal data in a certain way. A Job Applicant can withdraw such consent at any time though this may have consequences for the Trust's ability to continue to consider their candidature.

- To protect a Job Applicant's vital interests. This is applicable where a person's life could be at risk and the Trust needs to share or make available information to help them. This could involve sharing serious allergy information with staff, paramedics (or other medical professionals), or other information requested by the police or social services, to assist them in their enquiries to protect the individual.

- The Trust may also collect information about whether or not job applicants are disabled to make reasonable adjustments for candidates who have a disability. The Trust processes such information to carry out its obligations and exercise specific rights in relation to employment.

Storing Personal Data

Personal Data that the Trust collects as part of the job application process is stored in line with the Trust's Records Retention Policy. Personal data will be stored in a range of different places, including on an application record, in HR management systems and on other IT systems (including email). When it is no longer necessary the Trust will delete/securely destroy a Job Applicant's personal data and information in accordance with the Trust's current policies on the management of records.

How the Trust protects Personal Data

The Trust takes its security responsibilities seriously to protect personal data from accidental or unlawful access, disclosure, loss, damage or destruction. For example:

- Access to personal data is on a strict need to know basis
- Electronic records are held on encrypted servers
- The Trust has strict visitor management security procedures in place
- Sensitive paper files are locked away with restricted access to the keys
- The Trust's employees, volunteers and governors are subject to Disclosure and Barring Service (DBS) checks and employee contracts contain confidentiality clauses
- The Trust has policies, procedures and provides training covering data protection, security, record disposal and confidentiality.
- Encrypted email or secure file sharing platforms are used to share personal data with external

organisations

- Due diligence checks are undertaken on service providers and Data Protection Impact Assessments are undertaken, where required.
- Up to date virus and malware protection software is used; security patches are applied promptly and data is regularly backed up.

Sharing Personal Data

The Trust will not share information about a job applicant with third parties without their consent unless the law allows the Trust to. The Trust is required, by law, to pass on some of the personal data which it collects to:

- A Local Authority Designated Person/Safeguarding Leaders, when requested, for purposes of fulfilling their child safeguarding responsibilities
- Suppliers and service providers – to enable them to provide the service that the Trust has contracted them for e.g. HR and recruitment support
- Professional advisers and consultants
- Employment and recruitment agencies including online
- Medical occupational health professionals

Personal information may be shared internally for the purposes of the recruitment exercise. This includes members of the Trust's Executive Leadership Team involved in the recruitment process, interviewers involved in the recruitment process, senior leaders of a school and members of the Trust Board or the Local Governing Body and IT staff if access to the data is necessary for the performance of their roles also Internal Audit.

Consequences of not providing Personal Data

The Trust only asks a Job Applicant to provide personal data that it needs to enable it to make a decision about whether or not to offer a Job Applicant a role. If a Job Applicant does not provide particular information to the Trust, then the Trust will have to make a decision on whether or not to offer an individual a role without that information, which in some cases could result in the Trust deciding not to recruit an individual. For example, if the Trust asks a Job Applicant to provide an example of previous written work/ a certificate verifying a qualification and they do not, the Trust will have to decide whether to recruit an individual without that information. If a Job Applicant does not provide the Trust with names of referees or a reference when asked, the Trust will not usually be able to offer an individual the role.

In addition, some of the personal data provided by a Job Applicant to the Trust is required by law. For example, if a Job Applicant does not provide the Trust with the documentation it needs to check an individual's right to work in the UK, then the Trust cannot by law employ an individual.

If a Job Applicant chooses not to provide the Trust with personal data requested, the Trust will tell them about the implications of any such decision at the relevant time.

How long the Trust keeps Personal Data

The Trust will keep a Job Applicant's personal data throughout the recruitment process.

Should a job application be successful, when an individual starts to work for the Trust, another privacy notice will be provided that explains how the Trust processes an employee's personal data whilst working for the Trust.

If an application is unsuccessful, the Trust will keep personal data for up to six months from the date it notifies a Job Applicant if its decision. (Note, the Trust may keep personal data for longer than six months if a Job Applicant has asked the Trust to consider them for future vacancies – see 'Application held on file' below). There may, however, be circumstances in which it is appropriate for the Trust to keep particular items of a Job Applicant's personal data for longer. The Trust will base these decisions on relevant circumstances, taking into account the following criteria:

- the amount, nature, and sensitivity of the personal data
- the risk of harm from unauthorised use or disclosure
- the purposes for which the Trust processes the personal data and how long it needs the particular data to achieve these purposes
- how long the personal data is likely to remain accurate and up to date
- for how long the personal data might be relevant to possible future legal claims
- any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept

Application held on file

If a Job Applicant is unsuccessful for the role for which they have applied, or they sent the Trust a speculative application, then, if they have consented to the Trust doing so, the Trust will keep a Job Applicant's personal data on file to identify if they might be suitable for any other vacancies that may arise in the next two complete academic years and may contact a Job Applicant if it believes this is the case. The Trust will not keep a Job Applicant's personal data for this purpose for longer than two complete academic years.

Full details are given in the Trust's Records Retention Policy.

If during the period that the Trust has a Job Applicant's personal data on file, a Job Applicant may wish to apply for any particular vacancy that the Trust has open, and should contact the Trust to make it aware of this – particularly if it is not a close match with a Job Applicant's previous experience or is in a different area of the Trust from a vacancy applied for previously, as the Trust may not otherwise realise that the vacancy would be of interest to a Job Applicant.

When applying for a particular role, there is no obligation for a Job Applicant to consent to the Trust keeping their personal data on file for consideration for other roles if they do not want to. The application for the particular role a Job Applicant puts forward for, will not be affected.

If a Job Applicant changes their mind about the Trust keeping their personal data on file, they have the right to withdraw their consent at any time – see 'Your Rights', below.

References

If a Job Applicant provides the Trust details of referees, the Trust requires a Job Applicant to inform it what personal data of theirs they are sharing with the Trust. A Job Applicant must also give them the Trust's contact details and let them know that they should contact the Trust if they have any queries about how the Trust will use their personal data.

Automated decision-making

Recruitment processes are not based on automated decision-making.

Transferring Data Internationally

The Trust mainly stores data in the UK or the European Economic Area (EEA), however some of its service providers may store personal data outside these areas (usually in the USA). Where this is the case, the Trust has a contract with these service providers which ensures they process data securely and in line with UK data protection laws.

The Trust currently transfers personal data outside the EEA as it stores personal data on cloud systems based in the EEA that have backup systems that may sometimes be located outside the EEA.

Data Protection Rights

Job Applicants have the following rights under the data protection laws:

- To be told how their personal data is being processed – as outlined in this Privacy Notice.
- To request access to their personal information. This is known as making a 'Subject Access Request' (SAR). If a Job Applicant makes a subject access request, and if the Trust holds information about them, the Trust will:

- Provide a description of it
- Advise why it holds and processes it, and how long it will keep it for
- Explain where it got the personal data from, if not from a Job Applicant
- Advise who it has been, or will be, shared with
- Confirm if any automated decision-making is being applied to the data, and any consequences of this
- Provide a copy of the information in an intelligible form within a month, unless an extension is necessary on the ground of the complexity of the request

- To request that the Trust corrects incomplete or inaccurate personal data that it holds about a Job Applicant.

- To request that the Trust deletes or removes personal data that it holds about a Job Applicant where there is no good reason for the Trust continuing to process it. A Job Applicant also has the right to ask the Trust to delete or remove their personal data where they have exercised their right to object to processing (see below).

- To object to the Trust's processing of their personal data where the Trust relies on its legitimate interest (or those of a third party), where it cannot show a compelling reason to continue the processing

- To request that the Trust restricts its processing of personal data. This enables a Job Applicant to ask the Trust to suspend the processing of personal data about them, for example if they want the Trust to establish its accuracy or the reason for processing it.

- To withdraw consent to the Trust using personal data. As described above, the Trust does not normally rely on consent as the legal ground for using personal data. However, if it relies on consent as the legal ground for using any personal data and a Job Applicant withdraws consent, they also have the right to request that the Trust deletes or removes that data, if it does not have another good reason to continue using it.

Complaints/Concerns

The Trust takes any complaints about its collection and use of personal information very seriously.

If a Job Applicant thinks that the Trust's collection or use of personal information is unfair, misleading or inappropriate, or have any other concern/complaint about the Trust's data processing, they should raise this with the Trust's Data Protection Officer in the first instance - dpo@theictservice.org.uk

Alternatively, a Job Applicant can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113 (local rate)
- Call 01625 545 745 (national rate)
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact

If a Job Applicant would like to discuss anything in this privacy notice, please contact the Trust's Data Protection Officer - dpo@theictservice.org.uk