Workforce 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	24/5/18	-	1st issue
2	DPO	3/11/18	-	Add more organisations where personal data may be shared, withdrawal of consent
3	DPO	25/2/19	-	Add more organisations where personal data may be shared
4	DPO	14/6/19	-	Add more organisations where personal data may be shared
5	DPO	17/10/19	-	Photos and biometrics, Trust's tweets and website
6	DPO	8/1/20	-	CCTV added
7	DPO	10/6/20	-	Video conferencing software added
8	DPO	20/8/20	-	Covid-19 track and trace
9	DPO	25/11/20	17/12/20	Insertion of overview, withdrawal of consent right, why we collect personal data and the Trust's new address and change to the narrative on International transfers of data.
10	DPO	July 22	14/7/22	Many changes
11	DPO	6 March 2023		New DPO. Change of address of Data Controller

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.

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

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

The Trust may update this Privacy Notice at any time. This Privacy Notice does not form part of any contract of employment or other contract to provide services and the Trust may update this Privacy Notice at any time. It is important that employees read this Privacy Notice with any other policies mentioned within this Privacy Notice, so that they understand how the Trust processes their personal data and the procedures the Trust takes to protect their personal data.

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 an employee. Its address is Cromwell Community College, Wenny Road, Chatteris, Cambridgeshire, PE16 6UU.

The Trust's Data Protection Officer is The ICT Service - dpo@theictservice.org.uk. As Data Protection Officer, they are responsible for informing and advising the Trust about its data protection obligations and monitoring its compliance with these obligations. They also act as an employee's 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, employee 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

- personal information (such as name, address, date of birth, employee or teacher number, personal email addresses, and marital status);
- emergency contact information such as names, relationship, phone numbers and email addresses;
- characteristics information (such as gender and age);
- information collected during the recruitment process that the Trust retains during an employee's employment including references, proof of right to work in the UK, application form;
- nationality and immigration status and information from related documents, such as a passport or other identification and immigration information;
- employment contract information (such as start date, hours worked, post, roles and salary information);
- work absence information (such as leave, number of absences and reasons);
- education and qualifications (and, where relevant, subjects taught);
- training & development, online lesson recordings, performance records and professional memberships;
- payroll information (such as bank account details, remuneration, national insurance number, pension and benefits details & tax status information);
- details of any dependents;
- copy of driving licence;
- outcomes of any disciplinary and/or grievance procedures;
- images captured by CCTV footage at a school's premises and in any school - owned modes of transport etc;
- identity management/ authentication (such as photographs, for ID badges, or to identify an employee to the wider public via the Trust's or schools' websites and notice boards, to give pupils/students and parents/carers a clear picture of who is working at a school);
- use of a school's information and communications system including an employee's use of school-related social media;
- additional information required to complete the Department for Education's School Workforce Census, which includes details such as salary, qualifications and employment history.

The Trust may also collect, store and use sensitive personal data about an employee defined under the UK GDPR as “special category data” such as:

- race, ethnicity, religious beliefs, sexual orientation and political opinions;
- trade union membership (if an employee chooses to provide the Trust with this information;)
- health, including any medical information (such as disabilities, allergies and sickness records);
- biometric data – (e.g. finger print for cashless catering, printing, door entry and library management systems).

How the Trust collects employee personal data

The Trust collects personal information via application forms, new starter forms, contracts, change of personal details forms and by data collection forms; computer records; signing in/out records; from an employee’s passport or other identity documents such as their driving licence; from correspondence with an employee; or through interviews, meetings or other assessments (for example, team development/appraisals).

In some cases, the Trust collects personal data about an employee from third parties. This could be through the Home Office, the Trust’s pension providers, medical and occupational health professionals the Trust engages with, an employee’s trade union, and even other employees. References supplied by former employers and/or information from criminal records checks (known as DBS checks) permitted by law.

Information is also collected through CCTV, access control systems, biometric capture for the purposes of charging for meals; and any IT system a school has in place.

Workforce data is essential for a school’s / local authority’s operational use. While the majority of information the Trust collects from its employees is mandatory, some of it is requested on a voluntary basis. The Trust will inform an employee at the point of collection, whether an employee is required to provide certain information to the Trust or if an employee has a choice in this.

Why the Trust collects Personal Data

The Trust collects employee personal data to:

- enable individuals to be paid;
- enable the development of a comprehensive picture of the workforce and how it is deployed;
- maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency);
- inform the development of recruitment and retention policies;

- improve the management of workforce data across the Trust;
- allow better financial modelling and planning;
- enable gender, ethnicity and disability monitoring;
- facilitate safe recruitment, as part of the Trust's safeguarding obligations towards pupils/students;
- support effective performance management including planning for career development, and for succession planning;
- ensure the safety and welfare of its employees;
- inform the development of programs for continuing professional development;
- meet statutory reporting obligations;
- support pension payments and calculations;
- support the work of the School Teachers' Review Body;
- enable sickness monitoring;
- enable leave payments (such as sick pay and maternity leave);
- operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;
- provide references on request for current or former employees;
- facilitate virtual meetings via Microsoft Teams and Zoom.

Lawful Basis for collecting and processing Personal Data

The lawful basis the Trust relies on for processing employee personal data are:

- to meet the Trust's contractual obligations in relation to an employee's statement of employment contract with it.

- to satisfy the Trust's legal obligations and statutory duties as employer (such as The Health and Safety at Work Act, Equality Act 2010, The Disability Discrimination Act;

- to protect the vital interests of the data subject or of another natural person. 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 other employees, paramedics (or other medical professionals), or other information requested by the police or social services, to assist them in their enquiries to protect that person.

- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller e.g. The Education Act requires the collection of workforce data for the purpose of DfE's Census and its Working together to Safeguard Children Guidelines.

- legitimate interests pursued by the Controller or by a third party e.g. health and wellbeing providers

- consent has been provided by an employee

In addition, the Trust may process special category personal data in the following circumstances:

- with an employee's explicit written consent. This is usually applicable where the Trust asks for health, dietary information or biometric data (such as fingerprints).

- for performing any right or obligations which is imposed on the Trust in relation to employment, social security and social protection law (e.g. safeguarding individuals at risk; health & safety; protection against unlawful acts; prevention against fraud).
- it is necessary to protect the vital interests of any person where a person is physically or legally incapable of giving consent. This could be relied upon in situations where someone has become seriously ill on the Trust's premises and it is asked by medical practitioners (such as paramedics), to share information the Trust knows about that person's health or allergies.

- it is necessary for the establishment, exercise or defence of legal claims. The Trust may share or use special category data where legal action is being considered or underway.

- it is necessary in the substantial public interest. This may be relied upon in circumstances where the Trust's processing is necessary to safeguard children or others at risk or where it responds to requests from the Police or law enforcement bodies, to assist in an investigation to prevent or detect an unlawful act.

- is necessary for the assessment of the working capacity of an employee. This will be applicable where an employee has been absent from work due to illness or injury, and the Trust needs to assess whether they are fit to return to work.

Some of the reasons listed above for collecting and using an employee's personal data information overlap, and there may be several grounds which justify the Trust's use of an employee's data.

Withdrawal of Consent

Where the Trust processes an employee's personal data with their consent, an employee has the right to withdraw that consent at any time. The Trust will make this clear when requesting an employee's consent and explain how an employee goes about withdrawing consent if they wish to do so.

Once the Trust receives notification that an employee has withdrawn their consent, it will no longer process their information for the purpose or purposes an employee originally agreed to, unless the Trust has another legitimate basis for doing so in law.

Storing Personal Data

Personal Data that the Trust collects is stored in line with the Trust's Records Retention Policy. The personal information the Trust collects and stores is essential for the Trust's operational use. It only keeps personal information for as long as it needs to, and where it is necessary to comply with any legal, contractual, accounting or reporting obligations. After this period, the Trust deletes or securely destroys personally identifiable data.

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
- Strict visitor management security procedures in place
- Sensitive paper files are locked away with restricted access to the keys
- 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
- The Trust uses encrypted email or secure file sharing platforms to share personal data with external organisations
- Due diligence checks are undertaken on service providers and Data Protection Impact Assessments completed, where required.
- Up to date virus and malware protection software is used and security patches are applied promptly and data is backed up regularly.

Sharing Personal Data

The Trust may need to share an employee's personal data with third parties, including third party service providers where required by law, where it is necessary to administer the working relationship with an employee or where the Trust has another legitimate interest in doing so.

Department for Education (DfE) and Local Authorities
The Trust is required to share information about its workforce (this is known as the workforce census) to the DfE and Local Authorities so they can fulfil their statutory obligations relating to data collection and safeguarding under section 7 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

To find out more about the data collection requirements placed on the Trust by the DfE including the data that the Trust shares with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.
All data transferred to the DfE is sent securely and held under a combination of software and hardware controls which meet the current government security policy framework. To contact the DfE: https://www.gov.uk/contact-dfe

Why the DfE collects employee data
The workforce data that the Trust lawfully shares with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Sharing by the DfE
The DfE may share information about the Trust's workforce 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 DfE 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.

Other organisations where the Trust shares employee personal data

The Trust is required, by law, to pass on some of the personal data which it collects to:

- HMRC – The Trust shares an employee's identity and pay information with HMRC in conjunction with their legal obligation to pay income tax and make national insurance contributions.
- Pension Organisations – The Trust shares an employee's details with the employee's pension provider in order to make sure that they pay the correct amount and maintain an employee's entitlement to a pension upon their retirement. For teachers, the scheme is the TPS, for support staff the scheme is LGPS.
- Other schools within the Multi-Academy Trust - so the Trust can monitor and assess the quality and consistency of its services; share resources or to provide particular support to individuals. The Trust will only share identifiable information, where this is strictly necessary to enable it to carry out its official duties.
- Local Authority (in relation to their statutory or Child Protection duties and services)
- The Trust's HR and Payroll provider - (Education Personnel Management – EPM) – the Trust discloses details about an employee including national insurance number and absence information to enable an employee to be paid.
- Prospective employers in response to requests for employment references

In addition, the Trust may share employee information with:

- Educators and Examining Bodies
- An employee's family or representatives
- Data Barring Service
- Recruitment and supply agencies
- Professional bodies
- School trip organisations
- Suppliers and Service Providers to enable them to provide the service the

Trust has contracted them e.g. training providers
- Professional advisors such as lawyers and consultants
- Health authorities / Health and social welfare organisations / Occupational Health Providers
- Welfare services such as social services, LADO
- Salary sacrifice scheme – where an employee decides to become part of a salary sacrifice scheme such as that for child care vouchers, the Trust will share an employee's details with the provider to the extent necessary for them to provide the vouchers to an employee
- Software suppliers (data processors) to provide online teaching, learning and assessment, video conferencing software, parents/carers meeting booking system
- Survey and Research organisations
- Financial Organisations e.g. banks
- Trade unions and associations
- Ofsted inspector when they ask to see a sample of the Trust's records. These records could identify an employee. Any identifiable personal information the inspector may see, will not be taken away or used in their reports.
- Internal and External Auditors (e.g. Financial accountants/HMI Inspectors)
- Information Commissioner's Office (ICO) (complaints/breaches/ investigations)
- Law enforcement agencies and bodies (including Courts and Tribunals)
- Promotional Literature
- Press and the Media, Trust and school's websites and Social Media - only an employee's name and where consent has been received an employee's photo).

With an employee's explicit consent, the Trust will share information with:

- Credit reference agencies;
- Mortgage providers, Housing Associations and landlords

Transferring Personal 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.

How long the Trust keeps Personal Data

The Trust only keeps personal data for as long as necessary to fulfil the purposes it collects it for, as required to satisfy any legal, accounting or reporting obligations, or as necessary to resolve disputes.

Once an individual is no longer an employee, the Trust will securely destroy/delete personal information in accordance with its Records Retention Policy.

Data Protection Rights

An employee has the following rights under the data protection laws:

- To be told how their personal data is being processed (this Privacy Notice).

- To request access to their personal information. This is known as making a 'Subject Access Request' (SAR). If an employee makes a subject access request, and if the Trust holds information about an employee, it 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 have personal data rectified, if it is inaccurate or incomplete
- To request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- To restrict the Trust's processing of their personal data (i.e. permitting its storage but no further processing).
- To object to processing being used for public interest or direct marketing purposes (including profiling) and processing for the purposes of scientific/historical research and statistics

- To withdraw consent to processing, although the Trust may still continue to process an employee's personal data if a lawful basis other than consent applies.
- To have personal information, which an employee has provided, transmitted electronically to another organisation in certain circumstances.
- Not to be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect - unless an employee has agreed or in other limited circumstances
- Complain if they are not happy with the way their personal data has been handled, and to escalate this to the Information Commissioner if they remain dissatisfied.

Complaints/Concerns

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

If an employee thinks that the Trust's collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about the Trust's data processing, they should raise this with the Trust's Data Protection Officer in the first instance – email: dpo@theictservice.org.uk

Alternatively, an employee 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 an employee would like to discuss anything in this privacy notice, please contact the Trust's Data Protection Officer – email: dpo@theictservice.org.uk