Privacy Notice
Emergency Contact/Next of Kin

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	8/1/20	-	1st issue
2	DPO	12/7/18	-	cctv
3	DPO	20/8/20	-	Covid-19 track and trace
4	DPO	23/11/20	17/12/20	Overview, withdrawal of consent, international transfers, complaints
5	DPO	June 2022		Annual review – changes to be consistent with other privacy notices
6	DPO	6 March 2023		New DPO and 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.

The Trust collects and processes 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.

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 emergency contacts 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 obligations and monitoring its compliance with these obligations. They also act as an individual's first point of contact if they have any questions or concerns about data protection.

The Trust may need to update this privacy notice periodically if it changes how it collects and processes personal data.

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).

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

The personal data that the Trust may collect, use, store and share (where appropriate) about emergency contacts includes, but is not restricted to the following, which is provided by the parent/carer of a pupil or employee:

- Contact details (such as name, address, telephone and email)
- Relationship to the pupil or staff member and priority level of contact
- Any documentation given to the Trust on behalf of a pupil or employee regarding the relationship between the emergency contact and the pupil/employee.
- Images captured by CCTV on/adjacent to a school's premises

How the Trust collects Personal Data

The Trust collects personal information via the following methods:

- Pupil data collection forms / Admission Form
- Emails / text messages from parents and employees
- Employee appointment forms

The information provided to the Trust on a voluntary basis.

Why the Trust collects Emergency Contact Personal Data

The Trust has a legal duty to protect the safety and welfare of its pupils and its employees. It uses this data to:

- Contact a representative for the pupil in the event of serious incident involving a pupil where the main parent(s)/carer are not contactable
- Contact a representative of an employee in the event of serious incident involving an

employee
- Provide appropriate pastoral care for pupils
- Protect pupil welfare
- Comply with the law regarding pupil and employee welfare

Lawful Basis for collecting and processing Personal Data

- To comply with a legal obligation to pupils or employees
- To perform a task carried out in the public interest or in the exercise of official authority invested in the Controller
- To protect a child's or employee's vital interests

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.

Data Sharing

The Trust does not share personal information of emergency contacts with any external organisation. The information is solely used by staff employed by the Trust for emergency contact purposes only. However this may be shared in the following circumstance:

- schools that the student attends after leaving a Trust school.

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.

Transferring Personal Data Internationally

The Trust doesn't normally transfer personal information to a different country which is outside the European Economic Area (EEA). If this happens the Trust will be very careful to make sure that it is safe to transfer personal information and will look at whether that other country has good data protection laws for example.

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. Where the Trust transfers to a third party country or territory, it will do so in accordance with UK data protection law.

Data Protection Rights

An individual 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 individual makes a subject access request, and if the Trust holds information about an individual, 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
    - 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 personal data if a lawful basis other than consent applies.
- To have personal information, which an individual 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 individual 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.

Concern/Complaints

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

If an individual 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 at email: dpo@theictservice.org.uk

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