



Staffordshire University Academies Trust Personal Data Privacy Notice

Last reviewed	February 2026
Reviewed by	Operations Director
Approved by	CEO
Date of approval	February 2026
Policy owner	Operations Director
Location	Website

Our Trust and academies aim to ensure that all data collected about staff, pupils and students, parents and carers, LAC members and visitors is collected, stored and processed in accordance with the UK General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

This notice applies to all personal data, including data within both paper and electronic formats, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education.

Educational establishments who use personal data through the course of their duties, sector requirements and aims have a duty to inform individuals about how they collect and use their personal data, which can be provided through a privacy notice.

The Principles of Data Protection

The principles for data protection under the UK GDPR, and form the basis for how organisations are required to process personal information include that data shall be:

- Processed lawfully, fairly and in a transparent manner (Lawfulness)
- Collected for specified, explicit and legitimate purposes (Purpose Limitation)
- Adequate, relevant and limited to what is necessary (Data Minimisation)
- Accurate and, where necessary, kept up to date (Accuracy)
- Kept in a form which permits identification of data subjects for no longer than is necessary (Storage Limitation)
- Processed in a manner that ensures appropriate security of the personal data (Security and Confidentiality)

The principles also include the Accountability Principle which requires organisations processing personal information to take responsibility for complying with the other principles and how personal information is managed.

Lawful Basis

The data of individuals who are interacting with the academies and Trust is essential for our operation. The use of personal data helps us to meet our legal requirements, provide quality education to young people, support welfare and wellbeing, fulfil contracts, including contracts of employment.

Whilst the majority of personal information that is provided to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the UK GDPR, we will inform individuals at the point of collection, whether they are required to provide certain information to us to enable us to fulfil legal requirements and education sector specific duties, or whether consent is needed for us to collect and use personal information.

We only collect and use personal information about individuals when the law allows us to. Most commonly, we use it where we need to:

- Comply with a legal obligation (Article 6(1)c)
- Carry out a task in the public interest (Article 6(1)e)
- Legitimate interest (Article 6(1)f)
- Comply with a contractual obligation (Article 6(1)b)

Less commonly, we may also use personal information where:

- Individuals have given us consent to use it in a certain way (Article 6(1)a)
- We need to protect an individual's vital interests (Article 6(1)d)
- As a recognised legitimate interest under the Data Use and Access Act

We collect data which is specified under the UK General Data Protection Regulation as Special Category Data. This means that, under the UK GDPR, we have obligations to keep this data secure and use it where:

- We have explicit consent (Article 9(a))
- For employment, social security and social protection reasons (Article 9(b))
- Where we need to protect the vital interests of an individual (Article 9(c))
- We have a legitimate interest as a not-for-profit organisation (Article 9(d))
- For the safeguarding of children and individuals at risk (Paragraph 18, Schedule 1, Data Protection Act 2018)
- Health or social care (Article 9(h))
- Archiving and statistics (Article 9(j))

We will only use personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If personal information is required for use for a lawful but unrelated purpose, individuals shall be notified and the legal basis which allows us to process this information shall be shared.

Personal Information

We hold Personal and Special Category Data about individuals.

The personal data that we collect about staff, volunteers and job applicants helps us to:

- Improve the management of workforce data across the sector
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Comply with safer recruitment practices and legal obligations to keep children safe in education
- Allow better financial modelling and planning
- Enable staff to be paid in accordance with their contract of employment
- Enable equalities monitoring
- Support the work of the teachers' review body (where relevant)
- Ensure staff and children are safe in the workplace
- Support the wellbeing and welfare of staff in the workplace
- Make reasonable adjustments where necessary
- Support effective performance management and facilitating professional development
- Enable the monitoring of selected protected characteristics
- Carry out research
- Maintain security on the premises to safeguard staff and children
- Personnel management including retention, sickness and attendance
- Manage internal policy and procedure
- Human resources administration including pensions, payroll and benefits
- Determine qualifications for a particular job or task, including decisions about promotions
- Evidence for possible disciplinary or grievance processes
- Adhering to legal obligations
- To monitor and manage staff access to our systems and facilities in order to protect our networks, the personal data of our employees and for the purposes of safeguarding
- To monitor and protect the security of our network and information, including preventing unauthorised access to our computer network and communications systems and preventing malicious software distribution
- To respond to insurers in respect of any insurance policies which relate to you, and pursue claims
- Arrangements for the termination of the working relationship
- To meet health and safety obligations
- For the prevention and detection of fraud or other criminal offences
- To defend the Academy in respect of any investigation or court proceedings and to comply

with any court or tribunal order for disclosure

For governance professionals this helps us to:

- Comply with safer recruitment practices and legal obligations to keep children safe in education
- Enable governors to work with us and to take part in appropriate training and professional development
- Ensure staff and children are safe in the workplace
- Maintain security on the premises to safeguard staff and children
- Meet health and safety obligations including ensuring that appropriate access arrangements can be provided for individuals who require them
- Establish and maintain effective governance
- Meet statutory obligations for publishing and sharing governor details
- Support the operational functioning of the Trust and academies under the requirement as a public body organisation
- To keep governors up to date with news about the academies and the Trust
- To update mandatory databases
- To review governance within the Trust
- To comply with legal and regulatory requirements and liaise with regulatory bodies

For our parents / carers and learners this helps us to:

- Provide children with an education
- Get in touch with parents / carers as required, including for emergencies
- Support learning by keeping track of educational progress, monitor and report on pupil attainment progress, check how pupils are performing in exams and ascertain whether further help is required
- Ensure that personal information is accurate
- Track how well academies are performing and assess the quality of our services
- Look after children's wellbeing and provide appropriate pastoral care, to safeguard the welfare of children
- Offer family support, within the remit of the academies and Trust
- Keep children safe by collecting medical information, information regarding allergies, and provide appropriate medical care
- Ensure that pupils are safeguarded from harm and ensure their welfare is protected
- Keep school sites secure
- Ensure that we have a record of consents
- Meet statutory duties, including those placed upon us by the Department for Education
- Administer admissions waiting lists
- Carry out research to support teaching and learning
- Resolve any complaints or grievances
- Enable products to be purchased such as tickets for events, uniform, school meals, process free school meals
- Support research and for historical purposes for example, if a news article was written about an academy or the Trust
- To facilitate and deliver school meals
- To deliver interventions and offer further support and care

For visitors and contractors this helps us to:

- Ensure staff and children are safe in school;
- Maintain security on the premises to safeguard staff and children;
- Adhere to statutory guidance;
- Ensure health and safety procedures are followed;
- Conduct any work that the contractor has been contracted for.

For students on work placement this helps us to:

- Comply with legal obligations to keep children safe in education;
- Ensure staff and children are safe in the workplace;
- Maintain security on the premises to safeguard staff and children;
- Meet health and safety obligations including ensuring that appropriate access arrangements can be provided for individuals who require them;
- Establish and maintain effective teaching and learning;
- Permit the placement to take place successfully and support students during their placement;
- Support the operational functioning of the academy under its requirement as a public body organisation.

Individual Rights

Under the UK GDPR, individuals have specific rights over their personal data; this includes:

- The right to access personal data held about them (the right of subject access)
- The right to be informed about how and why their data is used
- The rights to have their data rectified, erased or restricted in certain circumstances
- The right to object in certain circumstances
- The right to portability of their data to another organisation
- The right not to be subject to a decision based solely on automated processing.

Individual rights can be exercised by contacting the academy or the Trust central team via the contact details on the website/s of the setting which is processing your personal information. We will process subject access requests in accordance with ICO guidance and our subject access request procedure.

Data Retention and Collection

The majority of data that we collect and process will be obtained directly from the data subject, or someone authorised to provide data on their behalf (e.g. a parent / carer with PR, on behalf of their child). Some data will be collected / obtained directly from third parties for example, for staff, references from previous employers or for children, from the previous school.

We hold data in accordance with our Retention and Records Management Policy which details how long we keep personal data for. Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely or rectified. We are required to keep certain data about individuals when they are no longer working at or with an academy or within the Trust, where required by law or where there are specific purposes for the information to be kept as detailed within our policy.

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. We may share data with third parties where there is consent to do so, unless the law, ICO guidance and our policies allow us to do so.

We are required, by law, to pass certain information about individuals to specified external bodies, such as our local authority and the Department for Education, so that they are able to meet their statutory obligations.

The Personal Data We Collect

The personal data that we collect for different parties includes (but may not be limited to) the following.

Job Applicants:

- Name, address, date of birth, gender, contact telephone number and email address
- Teacher number, QTS, DfES reference number, previous teaching experience (where relevant)
- National insurance number

- Employment history
- References (name, contact information, and written reference)
- Qualifications and where relevant, subjects taught
- CPD and training (including course name, awards, date of attendance)
- Data relating to warnings
- Data relating to child protection and safeguarding incidents
- Whether you have any prosecutions pending
- CCTV (if CCTV is based within a setting)
- Whether applicants have a driving licence, and any points on the licence
- Information about any incidents or issues that have happened and are publicly available online
- Race, ethnicity, religious beliefs, sexual orientation
- Health, including any medical conditions, physical and mental health information, and sickness records
- Data relating to disability
- Demographic information required for monitoring equal opportunities
- Criminal data, provided as part of our recruitment process application
- Time on and off site (signing in books and records)

Governance Professionals:

- Name, address, date of birth, contact telephone number and email address
- Role application details
- Employer / references (name and contact information)
- Time on and off site, CCTV, vehicle registration (whilst onsite)
- DBS number and date
- Identification
- Training and competency / skills matrix
- CPD (including course name, awards, date of attendance)
- Data relating to child protection and safeguarding incidents
- Criminal offence data
- Governance information – business and pecuniary interests, section 128 check, role, start and end date, meeting attendance records, records of communications, a biography which may be published on the website or in school, notes of meetings that attended
- Photograph (for the Trust's website)
- Monitoring data about the use of the information and communications system
- Call recordings (where activated)
- Data relating to disability and health data (where required to support access to site and manage health conditions)
- Demographic information required for monitoring equal opportunities
- Criminal data, provided as part of our recruitment process application
- Time on and off site (signing in books and records)
- Vetting including DBS data
- Vehicle registration

Parents / Carers and Learners

- Parent / carer and learners' contact details, such as name and address
- Parent / carer phone number and email address
- Date of birth and gender of learners
- Unique pupil number
- Details for emergency contacts – parent / carer / emergency contact details including name and address, phone number and email address
- Child's first language
- The child's position in the family, e.g. eldest sibling
- Admission number, the date of admission and the date of leaving, where appropriate
- A child's characteristics, such as ethnic background, religion, any special educational needs

- Eligibility for free school meals
- Parent's National Insurance Number (where required to provide free school meals)
- Identification (e.g. birth certificates)
- Any medical conditions a child has, including physical and mental health (such as doctor's information, child health, dental health, allergies, medication and dietary requirements), medicine consent and administering records
- Family circumstances which might affect a child's welfare or happiness
- A child's attendance records (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- National curriculum and agreed syllabus record sheets and religious education locally agreed syllabus sheets
- Workbooks and planners
- Written educational reports
- Special educational needs information
- A child's test results, attendance assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Safeguarding information (such as court orders and professional involvement, any notes indicating child protection disclosures and reports)
- Agency reports such as speech and language therapists, educational psychologist
- Any information about an education and healthcare (EHC) plan and support offered in relation to the EHC plan, or pre statutory support
- Individual risk assessments and care plans
- Notes relating to incidents and accidents that involve a child
- Any correspondence with parents/carers or external agencies including meetings and phone calls, emails
- Parental and, where appropriate, pupil consent forms for educational visits, photographs and videos, etc.
- Notes indicating that records of complaints made by parents/carers or the pupil are held
- Photographs of a child, to show prospective parents and pupils what we do at the Academy, to advertise the Academy, to celebrate good news stories and events
- CCTV images (if taken in the setting)
- Biometric information (if taken in the setting)
- Court orders or criminal petitions which relate to parents / carers and are required for safety and safeguarding reasons
- Information surrounding complaints or grievances
- Financial information
- Call recordings to school (where activated in the particular setting)
- Time on and off site (signing in books and records)
- Information about the use of our IT, communications and other systems, and other monitoring information
- Financial details
- Post 16 learning information

Staff Members

- Name, address, date of birth, gender, contact telephone number and email address
- Employee / teacher number
- Employment history
- References
- National insurance number
- Qualifications and where relevant, subjects taught
- Means of identification
- Pre-employment vetting including DBS data
- Right to work information
- Vehicle registration

- Driving licence (if the member of staff is required to drive for work purposes, or for identification)
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information
- Marital status
- Emergency contact information
- Contract and payroll information including timesheets, bank details, start date, hours worked, post, roles, salary information, maternity/paternity pay records, pension information
- Work absence information including the number of absences and reasons for absence
- Professional development information including performance management and appraisals, training records, lesson monitoring data
- Disciplinary information
- Recordings on video conferencing platforms
- Details of your use of business-related social media
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within the School, you will be notified separately if this is to occur)
- Information relating to accidents and incidents on site
- Where you leave employment and the reason for leaving is determined to be ill health, injury or disability and the records relating to that decision, including information needed for pensions
- Any health information in relation to a claim made under the absence insurance scheme
- Risk assessments
- Data relating to mental health and wellbeing including referrals to occupational health and other support services
- Data relating to warnings
- Data relating to child protection and safeguarding incidents, including those reported by the member of staff
- Childcare vouchers payment information (where relevant)
- CCTV (where active on site)
- Staff photos for identification purposes or where consent is provided to share this on Academy websites, social media platforms, displays
- Monitoring data about the use of the Academy's information and communications system
- Vetting including DBS data
- TUPE information (where relevant)
- Call recordings to and within school (if taken)
- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, physical and mental health information, and sickness records
- Biometric data (where active on site)
- Demographic information required for monitoring equal opportunities
- Criminal data, provided as part of our recruitment process application
- Data relating to disability
- Health, including any medical conditions, physical and mental health information, and sickness records
- Time on and off site (signing in books and records)

Visitors and Contractors

- Name
- Organisation
- Telephone number
- Time on and off site
- DBS number and date (where relevant to the reason for the visit)

- Identification
- Vehicle registration
- CCTV (if used in the setting)
- Training and competency (where relevant to the reason for the visit)
- Monitoring data about your use of the Academy's IT system
- Call recordings to school (if activated)
- Any accessibility requirements
- Photographs (upon signing in)
- Information relating to accidents and incidents on site
- Data relating to child protection and safeguarding incidents

Volunteers

- Name, address, date of birth, gender, contact telephone number and email address
- References
- Means of identification
- Vetting including DBS data
- Vehicle registration
- Emergency contact information
- Information relating to accidents and incidents on site and individual risk assessments
- Data relating to child protection and safeguarding incidents
- CCTV (if active within the setting)
- Volunteer photos
- Monitoring data about the use of the Academy's information and communications system
- Call recordings to school (if activated)
- Data relating to disability, health records including medical conditions
- Criminal data, provided as part of our safer recruitment processes
- Time on and off site (signing in books and records)

Placement Students

- Name, address, date of birth, gender, contact telephone number and email address
- Vetting including DBS data
- Vehicle registration
- Emergency contact information
- Information relating to accidents and incidents on site
- Data relating to child protection and safeguarding incidents
- CCTV (if active within the setting)
- Student photos
- Monitoring data about the use of the Academy's information and communications system
- Call recordings to school (if activated)
- Data relating to disability, health records including medical conditions
- Criminal data, provided as part of our safer recruitment processes

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you have any queries in relation to our processing, or think that our collection or use of personal information is unfair or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance by contacting our Data Protection Officer, following the guidance within the Complaints Policy on the Trust website (www.suatrust.co.uk):

Email – DPO@suatrust.co.uk

Telephone – 01782 987120

Alternatively, you can make a complaint to the Information Commissioner's Office after following our Complaints Policy:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Definitions

Personal data

Data from which a person can be identified, including data that, when combined with other readily available information, leads to identification of a person.

Special Category Data

The UK GDPR singles out some types of personal data as likely to be more sensitive, because use of this data could create significant risks to the individual's fundamental rights and freedoms. This includes:

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious or philosophical beliefs
- Personal data revealing trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health
- Data concerning a person's sex life
- Data concerning a person's sexual orientation.

Data Subject

The person whose personal data is held, used or processed.

Data Controller

A person or organisation that determines the purposes for which, and the manner in which, personal data is processed.

Data Processor

A person or organisation who processes the data on behalf of the data controller for specific purposes.