

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 1 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

## Data Protection Policy

Staffordshire University Academies Trust (SUAT) is required to process information about its staff members, pupils and other stakeholders. Organisations are required to process personal identifiable information in accordance with its legal obligations under the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018). This policy has due regard to the [DfE's Data Protection in Schools Guidance 2023](#) and the Information Commissioner's Office (ICO) guidance. The Information Commissioner's Office is the independent supervisory body regarding the UK's data protection legislation.

Data protection is about regulating the way that organisations who use and store personal identifiable information about people (personal data), and it provides individuals with various rights regarding the use of their data. SUAT processes personal data including information about its members, directors, staff, pupils/students, Local Academy council members, volunteers, parents/carers, suppliers and other third parties. It recognises that the correct and lawful treatment of personal data is crucial in maintaining confidence in SUAT and in how it operates both through its business and educational functions within the public sector.

This policy is applicable to all people working in SUAT (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities because the correct, lawful and moral treatment of personal data applies to all individuals working within SUAT.

This policy is in place to ensure all staff (including volunteers), Local Academy Council and Trust Board members are aware of their responsibilities and outlines how the Trust and the Academies comply with the principles and requirements of the UK GDPR and DPA 2018.

### 1. Legal framework

1.1 This policy has due regard to legislation, including, but not limited to the following:

- The UK General Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000 (FoIA 2000)
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Data Protection Act 2018
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2 This policy will also have regard to the following guidance: Information Commissioner's Office 'Guide to the UK General Data Protection Regulation.' IRMS Academies Toolkit.

1.3 This policy will be implemented in conjunction with (but not limited to) the following policies:

- Compliant Records Management Policy (Data Retention)
- IT Acceptable Use Policy
- Freedom of Information Policy (parts A and B)
- CCTV Policy

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 2 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

- Safeguarding Policy
- E-Safety Policy
- Use of Images Policy
- Information Sharing Policy
- Information Security Policy
- Privacy Notices

## 1.4 Responsibilities

The Trust and Academies are the data controller and have a corporate and moral responsibility to comply with data protection legislation. All users of personal data within the Trust and Academies have a responsibility to ensure that personal data is always held securely and not disclosed to any unauthorised third party either accidentally, negligently or intentionally. Everyone is responsible for protecting personal data.

For most of the personal data that is collected, stored and used, the Trust and Academies are the data controller. This means that we are responsible under the Data Protection Act 2018 for protecting data in every situation where our organisation decides:

- Whose information to collect
- What types of data is required to function to permit our organisation to function in accordance with our official duties as a public sector organisation
- The reasons that this data is needed
- Whether the information can be shared with a third party or third parties
- When and where data subjects' rights apply
- How long to keep the data for

The Trust is registered with the Information Commissioner's Office, reference ZA286224.

In certain circumstances, the role of the data controller may also be extended to third parties, for example, when the organisation is required to supply a copy of some personal data to the Department for Education (DfE), DfE also becomes an independent data controller of the copy it receives.

All employees, volunteers and others accessing and processing personal data of the Trust or Academies must adhere to data protection policies and code of conduct, keep all personal data secure throughout its lifespan and participate in relevant data protection inductions and training.

Trustees and Local Academy Councils:

- Monitor their data protection performance
- Support the Data Protection Officer and senior leaders
- Have good network security infrastructure to keep personal data protected

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 3 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

- Have a business continuity plan in place that includes cyber security / or have a cyber response plan held separately to the business continuity plan

The person within each Academy designated as the 'responsible person' for data protection, or 'Data Protection Lead', and the Academy Principal, will be responsible for ensuring and monitoring compliance with Trust data protection policies, and reporting as required to the DPO, including:

- Ensuring that all personal data is kept securely and security management measures are sufficient
- Maintaining records relating to data protection, including all actions and decisions relating to data protection matters, subject access requests, information asset registers, potential breaches, requests made in relation to personal data, records of processing activities
- Ensuring that personal data is kept in accordance with the Trust's retention schedule
- Ensuring that queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO as necessary
- Ensuring that any data protection breaches are swiftly brought to the attention of the Data Protection Officer in adherence with the Personal Data Breach Management Plan and that they support the DPO in investigating breaches
- Where there is uncertainty around a data protection matter, advice is sought from the DPO
- Providing the required training and inductions for staff or arranging this with the DPO, and ensuring that refresher training is undertaken annually
- Maintaining records of training
- Communicating with the DPO where a Data Protection Impact Assessment be required
- Supporting data protection audits

Senior leaders:

- Decide how the Academy uses technology and maintains its security
- Decide what data is shared and how, in conjunction with the Data Sharing Policy
- Set procedures for the use of data and technology
- Understand what UK GDPR and the Data Protection Act covers and obtain advice from the Data Protection Officer, as appropriate
- Assure LAC members and Trustees that their setting has the right policies and procedures in place / is following policies and procedures
- Ensure that staff receive annual training on data protection, including specific Trust and Academy processes such as personal data breach reporting processes and the escalation of information rights requests

All staff have responsibilities to ensure:

- All personal data is kept securely throughout its lifespan
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Personal data is kept in accordance with the Trust's retention schedule
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the responsible person at each Academy

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 4 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

- Any data protection breaches are swiftly brought to the attention of the responsible person and the Data Protection Officer and that they support the DPO in resolving breaches in accordance with the Personal Data Breach Management Plan
- Where there is uncertainty around a data protection matter advice is sought from the responsible person and DPO
- Training and inductions are attended, including annual refresher training
- Communicating with the responsible person where new processing activities are due to take place so that a DPIA can be considered and arranged
- Supporting data protection audits

All staff, including but not limited to teaching staff, catering staff, welfare supervisors, library staff, cleaning staff, first aiders, LAC members and Trustees, volunteers should be aware of what:

- Personal data is
- 'Processing' means
- Their duties are in handling personal information
- The processes are for using personal information
- Is permitted usage of that data
- The risks are if data gets into the wrong hands
- Their responsibilities are when recognising and responding to a personal data breach
- The process is for recognising and escalating information rights requests

There are extra requirements for any staff in school who create and store data, enter data into applications or software, decide if and when they'll process certain data and handle paper documents containing personal data. These staff members are responsible for:

- Making sure they have a legitimate need to process the data
- Checking that any data they store is needed to carry out necessary tasks
- Identifying any risks
- Understanding the governance arrangements that oversee the management of risks

Contractors, Short-Term and Voluntary Staff are responsible for ensuring:

- Any personal data collected or processed in the course of work undertaken for the Trust or Academies is kept securely and confidentially at all times
- All personal data is returned to the Trust or Academies on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and the Trust / Academies provide approval in this regard from the contractor or short term / voluntary member of staff. Evidence of destruction must be provided
- The Trust / Academies receive prior notification of any disclosure of personal data to any other organisation or any person, and approve this disclosure
- Any personal data made available by the Trust / Academies, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been given by the Trust/Academies

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 5 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

- All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly, that there is a lawful basis for providing them with that information, and that consent to process personal data is obtained where necessary.

## 2. Personal data

2.1 Personal data refers to information that relates to a living individual, who could directly or indirectly be identified through the processing of their personal data. This includes information such as an online identifier, for example an IP address.

2.2 The UK GDPR applies to electronic and automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data (where pseudonymisation enhances the privacy of data by replacing identifying fields within a data record by one or more artificial identifiers), e.g. key-coded. Examples of personal data are:

- Identity details; name, title, role
- Contact details; address, phone number
- A pupil report
- Pupil behaviour and attendance
- Assessment and exam results
- A contract of employment, staff recruitment information
- Staff development reviews
- Pupils'/students' exercise books, coursework and mark books
- Health records
- Email correspondence relating to an individual
- Governance records
- Payroll data
- Risk assessments

2.3 Sensitive personal data is referred to in the UK GDPR as 'special categories of personal data'. SCD is considered to be more sensitive and is given more protection in data protection law. Special category data includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (e.g. fingerprints)
- Data concerning health (mental and physical health) and medical records
- Data concerning a natural person's sex life or sexual orientation

In Academies, this will also include:

- Information concerning child protection matters and safeguarding
- Pupils in receipt of pupil premium

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>				
<b>Approved by:</b>	<b>Trust Board</b>	<b>Issue date:</b>	<b>May 2023</b>	<b>Review date:</b>	<b>May 2024</b>	
<b>Policy Owner:</b>	<b>DPO</b>	Page: 6 of 32				
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>

- Data relating to special educational needs and disability (SEND)
- Children in need and children looked after by a local authority

Criminal offence data is personal data that is treated in a similarly sensitive way to SCD; it records criminal convictions and offences or related security measures. Criminal offence data includes the alleged committing of an offence and the legal proceedings for an offence that was committed or alleged to have been committed, including sentencing.

SUAT and the Academies process criminal offence data in storing the outcome of a Disclosure and Barring Service (DBS) check on their employees, non-employed staff and volunteers. As this data relates to criminal convictions, collecting and retaining it means that we are processing criminal offence data. This applies even if a check has not revealed any conviction.

2.4 Academies collect, store and use personal data about a variety of individuals. Those individuals are known as the data subjects. Academy and Trust data subjects include:

- Pupils and former pupils
- Parents and carers
- Employees and non-employed staff
- LAC members and Trustees
- Volunteers, visitors and job applicants
- Work placement students

2.5 Academies hold personal data in several forms. These are known as data assets and data items and include:

- Data item groups – data items about the same process
- Data sets – collections of related data that can be manipulated as a unit by a computer
- Systems – administrative software
- System groups – the larger systems housing administrative software

### 3. Principles

3.1 The UK GDPR provides 7 principles of data protection. The principles of data protection lie at the heart of data protection laws and designate that personal data must be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals (Lawfulness, Fairness and Transparency Principle).
- Collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (Purpose Limitation Principle). Purposes shall be detailed within Academy information asset registers.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 7 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Data Minimisation Principle).
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Accuracy Principle).
- Kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals (Storage Limitation Principle). This will be managed in accordance with the Data Retention Policy.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Integrity and Confidentiality Principle). This will be managed in accordance with the Information Security Policy.

3.2 The UK GDPR requires that “the controller shall be responsible for, and able to demonstrate, compliance with the principles”. Processing activities shall be documented effectively. (Accountability Principle).

3.3 "Processing" covers virtually every aspect of a setting’s use of personal information from the point of collection and throughout its lifespan. Processing includes using, disclosing, copying, sharing, entering data into electronic and filing systems, storing and disposing of personal data.

3.4 Individuals must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in relation to their personal information, how long it is kept for and about their right to complain to the Information Commissioner’s Office (ICO), as the UK’s regulator for data protection and is the independent body that upholds the UK’s information rights. This information is provided in the SUAT’s privacy notices and can be obtained from the SUAT and Academy websites.

3.5 If Personal Data is being used in a way that is not compatible or not in compliance with data protection law, this must be raised with the DPL or DPO immediately.

#### 4. Accountability

4.1 SUAT and the Academies will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. This includes:

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 8 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

- The use of privacy notices; comprehensive, clear and transparent template privacy notices will be provided by the Trust for each setting to adapt accordingly. Privacy notices will be shared with data subjects and revised on a regular basis.
- Internal records of processing activities will include the following:
  - Name and details of the organisation
  - Purpose(s) of the processing
  - Description of the categories of individuals and their personal data
  - Retention schedules
  - Categories of recipients of personal data
  - Details of third parties using the data
  - Description of technical and organisational security measures
  - Information requests and details of how and when the request was responded to
  - Personal data breaches, how and when the breach was managed
  - The sharing of privacy notices and information
  - Consent obtained for the processing of personal data (this includes consent from parents / carers, secondary students and staff)
  - The compliant disposal of personal data at the end of its retention period, or legal reasons for keeping data beyond its retention period
  - Data protection impact assessments undertaken for processing personal data

4.2 The Trust and its Academies occupy a single registration with the ICO as the Data Controller. The Trust and its Academies retain a copy of the certification as a Data Controller and the registration is updated upon the joining of new academies to the Trust.

4.3 The Trust and Academies will maintain appropriate records in relation to their processing activities relating to personal data.

4.4 The Trust and Academies will maintain appropriate policies and procedures in relation to the processing of personal data, which shall be reviewed annually.

4.5 Individuals processing personal data during the course of their work for the Trust / Academies shall be appropriately trained in data protection and cyber security, according to the nature of their role and type of data that they are processing. Inductions relating to data protection will also be provided. All staff must learn about UK GDPR and data protection as part of their annual induction in the same way they learn about safeguarding.

## 5. Data Protection Officer (DPO)

5.1 A DPO is appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the UK GDPR, DPA 2018 and other such data protection laws.
- Monitor compliance with the UK GDPR, DPA 2018 and other such laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal reviews, and providing the required training to staff members.



Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 9 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

5.2 The role of DPO will be undertaken by the Operations Manager, provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3 The DPO will undertake training in relation to the UK GDPR and have knowledge of data protection law, particularly that in relation to Educational Establishments.

5.4 The DPO shall:

- Advise Academy leaders and staff about their data obligations
- Monitor compliance
- Conduct regular data audits
- Develop and update data protection policies, procedures, template documentation
- Provide advice regarding data protection impact assessments
- Answer, or support in answering data protection enquiries from staff, parents and pupils
- Ensure privacy notices are regularly reviewed and updated
- Support and advise staff who have data protection queries
- Communicate with the Information Commissioner's Office (ICO)
- Report to Trustees about data protection
- Advise Trustees on data protection risks
- Advise on and coordinate responses to information rights requests
- Review the security and managements of assets containing personal data

5.5 The DPO will report to the highest level of Trust management, which is the CEO, Deputy CEOs and Trust Board.

5.6 The DPO will operate independently and will not be penalised for performing their duties.

5.7 Sufficient resources and time will be provided to the DPO to enable them to meet their obligations.

## 6. Lawful processing

6.1 The legal basis for processing data must be identified and documented prior to data being processed. The DPO will be consulted where the Academy has a requirement to process new personal data fields.

6.2 Under data protection legislation, there are a number of justifications that permit personal data to be processed. The UK General Data Protection Regulation details 6 lawful bases on which personal data is permitted to be processed. At least one lawful basis for processing must apply. The organisation must choose the most appropriate lawful basis, which are as follows:

- The consent of the data subject has been obtained (or where an approved individual acting on their behalf provides consent). The individual concerned must have a real choice in the use of their data.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 10 of 32			
Audience:	Trustees <input checked="" type="checkbox"/> Parents <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	

- Processing is necessary for:
  - Compliance with a legal obligation, to permit the Academy / Trust to comply with the law.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Where the use of the data is necessary to permit the Academy / Trust to carry out a task in the public interest or its official functions, and that task or function has a clear basis in law.
  - For the performance of a contract with the data subject or to take steps to enter into a contract; the use of the data is necessary for a contract the Academy / Trust has or will have with the individual concerned.
  - Protecting the vital interests of a data subject or another person; where the use of the data is necessary to protect an individual's life.
  - Where use of the personal data is for the Trust / Academy or a third party's legitimate interest, except where such interests are overridden by the interests, rights or freedoms of the data subject.

6.3 If there is a need to process Personal Data that is not set out in the relevant privacy notice(s), it would be appropriate to contact the DPL/DPO to ensure that a lawful reason for using the Personal Data has been identified and documented.

6.4 Under UK GDPR, there are 10 additional conditions for processing SCD. At least one lawful basis and one condition must apply. The conditions are:

- Explicit consent – the accessing or processing of this personal data has the written consent of the individual concerned
- Employment, social security or social protection – it's necessary for one of these 3 stated purposes and authorised by law
- Vital interests – it's necessary to protect an individual's life
- Not-for-profit body – it's necessary for the legitimate internal-only purposes of a membership body with a political, philosophical, religious or trade-union aim
- Manifestly made public – it relates to personal data the individual has themselves deliberately made public
- Legal claims or judicial acts – it's necessary for a legal case or required by a court of law
- Substantial public interest – there's a relevant basis in UK law and one of the 23 specific public interest conditions has been met
- Health or social care – it's necessary for the provision of healthcare or treatment, or of social care, and there's a basis in law
- Public health – it's necessary for reasons of public interest, and there's a basis in law
- Archiving, research and statistics – it's necessary for reasons of public interest, and there's a basis in law

6.5 Criminal offence data is treated in a similar way to special category data. One of the 6 lawful bases must apply and the processing must also be covered by one of the conditions described in Schedule 1 of the DPA.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 11 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

6.6 The Data Protection Act 2018 (DPA), Schedule 1, Parts 1 and 2 has more information about the conditions that are authorised or have a basis in law. For conditions (b), (h), (i) or (j), the associated condition in UK law, set out in Part 1 of [Schedule 1 of the DPA 2018](#) also need to be met. For substantial public interest condition in Article 9(2)(g), one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018 also need to be met. The ICO's [lawful basis interactive guidance tool](#) can help organisations to decide whether they have the legal right to process particular personal data items and on what grounds.

## 7. Consent

- 7.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. The UK GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. For consent to be considered 'freely given', an individual must suffer no detriment if they refuse to give it.
- 7.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- 7.3 Where consent is given, a record will be kept documenting how and when consent was given. Copies of written consent will be maintained and securely stored.
- 7.4 Consent mechanisms are required to meet the standards of the UK GDPR. Consent cannot be utilised as a lawful basis for processing where the data must be processed in order for the Trust or Academies to fulfil their functions as a public body, where there is a legal or contractual obligation to process the data, or where processing falls under vital or legitimate interests. In short, consent will not be appropriate where it is necessary to process the data and the individual cannot be given a real choice.
- 7.5 Consent can be withdrawn by the individual at any time and following the withdrawal of consent, the processing will cease. Where consent is withdrawn, all relevant parties who process the fields of personal data for which the consent is withdrawn shall be informed by the designated employee / Data Lead.
- 7.6 If consent is required, it must be obtained in writing at the point of data collection. Individuals will be informed how to withdraw their consent at the point of collection and via Privacy Notices.
- 7.7 The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child, or where the child meets the minimum age of consent as defined in the UK GDPR. In the case of a conflict of consent, e.g. where the child's parents are separated but with joint custody, the consent may be determined by the child, so long as the child understands the impact(s) of providing their consent.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 12 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

7.8 It is recognised that where consent is provided on behalf of a child, the personal data still belongs to the child and the child may withdraw their consent where they have sufficient understanding and maturity of the terms of the nature and implications of providing and withdrawing consent, to enable them to do so. Children who are mature enough to understand the implications of providing consent for the processing of their personal data will be able to give their own consent.

7.9 Individuals should give written consent wherever possible. Consent should be requested after the individual has been fully informed about how the personal data will be used.

7.10 Queries regarding consent should be raised with the DPO / DPL.

7.11 The Academy / Trust cannot continue to process personal data indefinitely. This should be processed in accordance with the retention policy and storage limitation principle of the UK GDPR, and not retained for longer than is required to fulfil the original purpose for using the data. Where an individual never withdraws consent, the Trust / Academy must still adhere to the retention policy and storage limitation requirements.

7.12 Consent should be refreshed at regular intervals, and individuals reminded of the procedure for withdrawing their consent, upon providing this.

## 8. Privacy Notices and the Rights of Individuals

8.1 Under UK GDPR and the Data Protection Act 2018, every Academy has to make its privacy notices freely available to those whose personal data it handles.

8.2 A privacy notice explains:

- Why an Academy / Trust needs to collect personal data
- Who the Data Controller is
- What data is being processed
- What it plans to do with the data
- How long it will keep the data
- Whether it will be sharing the data with any other organisation and why
- What the lawful basis is
- How individuals can exercise their rights over their personal data
- Who to contact if an individual has any concerns

8.3 Privacy notices are required to be clear and accessible. Privacy notices are updated based on DfE model privacy notices and shall be reviewed regularly and updated where there are any changes to processes surrounding the use of personal data. The ICO has a useful checklist of [what to include in a privacy notice](#).

8.4 Privacy notices shall be tailored to each setting and upon any changes or updates to privacy notices, they shall be re-shared with data subjects.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 13 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

8.5 Privacy notices will remain accessible via Trust and Academy websites and will be provided for individuals at the point of data collection.

8.6 The rights of data subjects are:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

8.7 It is important to recognise that children have the same rights over their personal data as adults.

8.8 Sections 9 to 16 of this policy provide further details regarding the rights of individuals in relation to the processing of their personal data. Individuals, including children, have several information rights relating to personal data held about them. This includes the right to:

- Request access to the personal data you hold about them by raising a subject access request
- Change personal data that is held about them, particularly where it is inaccurate or incomplete
- Remove their personal data from record, particularly where it is no longer required, consent has been withdrawn or it has reached the end of its retention period
- Restrict the processing of their personal information
- Stop the processing of their personal information (right to object)

8.9 Information rights requests relating to personal data can be made verbally or in writing, including via social media. Unless there's a valid reason, an information rights request must be responded to within one calendar month. If the case is complex, the response deadline can be extended by an extra two calendar months.

8.10 Information rights requests only apply to the personal data that the Academy / Trust holds when they receive the request.

8.11 All staff must be trained to recognise different kinds of information rights request and know how to escalate a request if they receive one.

## 9. The Right to be Informed

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 14 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

9.1 Individuals have the right to be informed regarding how their data is used. The Trust and Academies will use Privacy Notices (in accordance with section 8 of this policy) to inform individuals about the use of their data.

9.2 Privacy notices will be written in clear, plain language which is concise, transparent, easily accessible, free of charge and can be easily understood by the relevant party, this includes privacy notices provided for pupils and students.

9.3 Data should be obtained directly from the data subject wherever possible but in some circumstances, data may need to be requested from third parties, for example, references from previous employers, Occupational Health reports and health care plans.

9.4 Privacy notices should inform individuals where their data will be sought from third parties, who the third parties are and the legal basis for obtaining information in this format.

9.5 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

9.6 Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

9.7 In relation to data that is not obtained directly from the data subject, this information will be supplied, where relevant to do so:

- Without undue delay, following receipt of the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

## 10. The Right of Access

10.1 Individuals have the right to obtain confirmation that their data is being processed, to check the lawfulness of the processing and to request copies of their personal data. The Trust has a Subject Access Request procedure for use by Academies, to support the management of such requests. Requests may be received from parties including:

- A parent or carer wishing to see what data is held about themselves or their child
- A / student pupil wishing to see their educational record or a breakdown of their exam marks and the marker's comments
- Staff
- Former staff or pupils
- A solicitor on behalf of a pupil, parent or carer, or staff member

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 15 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

10.2 Individuals can submit a subject access request (SAR), to request access to their personal data that is processed by the Academy / Trust, by contacting the individual Academy's Data Protection Lead, or the DPO. The contact details for each DPL and the DPO are contained on Academy and Trust websites and within privacy notices.

10.3 The SAR must be made in writing, by the data subject, or an approved representative on their behalf, wherever possible. Where the SAR cannot be made in writing, suitable adjustments must be made to ensure that the request can be made, and without undue delay.

10.4 The scope of the information which the individual wishes to access must be precise, to allow the Academy / Trust to identify, collate the review the information requested and prevent delays in responding to the request.

10.5 The request should be made directly with the individual Academy/Trust that processes the information, and must include the name and contact details of the requester, alongside clear and accurate details of the data the individual is requesting, and the time frame to which the data relates. A SAR cannot be processed without this information.

10.6 The Trust/Academy will verify the identity of the person making the request, by suitable means, before any information is supplied. Suitable means will depend on various factors including how well known the individual is to the Academy/Trust and what data is processed about them. Information can only be provided once the verification of the data subject's identity has been made.

10.7 If a request is made by a third party on behalf of a data subject, the data subject must provide written consent for the third party to act on their behalf.

10.8 All requests will be acknowledged as soon as possible. Subject access requests will be responded to without undue delay but within one calendar month, unless an extension is required. Extensions may be applied where a request is considered to be complex. Where an extension is required, this will be assessed and agreed by the DPO in conjunction with the ICO's criteria for extending response times, and the decision will be recorded in writing. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one calendar month of the setting receiving the request.

10.9 In responding to subject access requests, the Trust/Academy will be required to consider whether any exemptions apply to the request. Where an exemption is identified, it will be applied to the subject access request and will inform the information that is provided in response to the request. Individuals will be informed if an exemption applies, and this will be recorded by the Academy/Trust.

10.10 Before responding to a subject access request raised by a parent or carer about a child, checks must be made to verify:

- Whether the requester has parental responsibility for the child
- Whether the child is aged 13 or older, and if so, whether they have given their consent for a parent or carer to act on their behalf

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024
<b>Policy Owner:</b>	DPO	Page: 16 of 32			
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

- Whether releasing the information to an absent parent or carer would cause the child distress or result in safeguarding concerns

**The impact that releasing the data would have on the child and their wellbeing must be considered before a response is made.**

A pupil's educational record will not be provided to a parent or carer if there is a court order in place that limits the exercise of their parental responsibility.

The Information Commissioner's Office has more information about [accessing pupils' information](#).

10.11 In the event that the requested data includes personal information of any third parties, the Trust/Academy will consider whether providing the information would prejudice the rights of such parties and how their personal data will be adequately protected. Protection may be made through redacting third party data, where the individual cannot be further identified through the redaction, or by gaining written consent from the individual to issue their data in response to the subject access request.

10.12 Where the response to the subject access request risks adversely affecting any third parties whose personal data is contained within the request, and this cannot be adequately redacted without still being able to identify the individual, the data required in response to the subject access request may not be issued in part or in full, the DPO will consider whether an exemption applies.

10.13 The copy of the information supplied will be free of charge to the individual, however, the Trust / Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information. All fees will be based on the administrative cost of providing the information.

10.14 Academy/Trust will provide the information in a format which is deemed suitable in accordance with the format in which it is stored, for example, electronically stored files may be sent in a PDF format.

10.15 Any personal information provided in response to a subject access request must be issued in a secure format.

10.16 Where a request is deemed manifestly unfounded or excessive by the DPO, the Academy/Trust holds the right to deny the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one calendar month of the request.

10.17 Where a request for information is made on behalf of an individual by a third party, the Academy/Trust must be satisfied that the third party is entitled to act upon behalf of the individual; it is the responsibility of the third party to provide written confirmation of entitlement. If the Academy/Trust feels that the individual to which the personal relates may not understand what information will be issued to the third party, the Academy/Trust may issue the personal data directly to the individual to decide whether to share such data with the third party.



Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 17 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

10.18 Where a request for information is made on behalf of a child, the Academy/Trust recognises that the personal data belongs to the child and the rights and freedoms of the child must not be adversely affected. The Academy/Trust will therefore consider:

- The child's wellbeing;
- Legislation which may affect such requests;
- The child's level of maturity and their ability to make decisions of this nature;
- The nature of the personal data;
- Any court orders relating to parental access or responsibility that may apply;
- Any duty of confidence owed to the child or young person;
- Any consequences of allowing third parties, including those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations relating to safeguarding;
- Any detriment to the child or young person if third parties or individuals with parental responsibility cannot access this information; and
- Any views the child or young person has on whether third parties or those with parental responsibility should have access to information about them.

SUAT recognises that certain personal information relating to a child must be shared with parents and carers to allow the Trust and its Academies to fulfil such duties as a public sector organisation.

10.19 A brief outline of the subject access procedure is detailed below. Academies can access the full procedure via Teams.

- Log the request and report to the DPO. Keep a log of any actions and decisions made in relation to the request.
- Check the identity of the requester and their right to request the data. If a parent or carer is making the request on behalf of a pupil aged 13 or over, check they have consent.
- Make sure it is clear from the request exactly what personal data the individual wants. Ask for clarification if you need to.
- Acknowledge you've received the subject access request as soon as possible. Tell them when you'll send the response.
- Consider if the subject access request is complex. If you need another 2 months to produce the information, make sure you've told the requester within one month of receiving the request. You must explain why you need the extra 2 months and this must be in consultation with the DPO.
- Before you send over any data, check if any information in the files needs to be redacted – for example, if it refers to other people.
- Check whether any exemptions apply.
- Send the final response and securely transfer the requested information to the individual.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 18 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

10.20 Keep a record of any subject access requests, including:

- The request itself
- The date you received it
- All correspondence relating to the request (you should not keep personal documents used to confirm identity)
- What you provided
- When you provided it
- Confirmation that the requester received the data in question
- Details of your decision-making rationale in case of challenges

10.21 The Information Commissioner's Office has a [step-by-step guide to help you deal with a request for information](#).

## 11. The Right to Rectification

11.1 Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2 The Academy / Trust must be satisfied of the identity of the individual requesting the rectification, prior to making the rectification, and that they are approved / entitled to make the changes that have been requested, for example, a parent requesting a change to a child's address has Parental Responsibility.

11.3 Where the personal data in question has been disclosed to third parties, the Trust / Academy will inform them of the rectification required, e.g. updating the data on the management information system.

11.4 If required, the Trust / Academy will inform the individual about the third parties that the data has been disclosed to who will be required to rectify the data they process.

11.5 Requests for rectification will be responded to within one month; this will be extended by up to two months where the request for rectification is complex, for example, if legal advice is required, or the request involves complex technical support. The individual will be informed of the extension and their right to complain to the supervisory authority within one month. The setting receiving the request must endeavour to make the changes without undue delay, on approval of the request

11.6 Where no action is being taken in response to a request for rectification, for example, because the requester does not have the authority to make the changes to the personal data, the Trust / Academy will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority.

11.7 The request will be recorded, along with actions and decisions undertaken in relation to the request.

## 12. The Right to Erasure

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 19 of 32			
Audience:	Trustees <input checked="" type="checkbox"/> Parents <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	

12.1 Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The Trust / Academy will verify the identity of the requester prior to erasing any data and ensure that they are permitted to make such a request.

12.2 Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

12.4 The Academy / Trust must be satisfied of the identity of the individual making the request, prior to erasing personal data, and that they are authorised to make the request.

12.5 Requests for erasure will be responded to within one month; this will be extended by up to two months where the request for erasure is complex, for example, if legal advice is required, or the request involves complex technical support. The individual will be informed of the extension and their right to complain to the supervisory authority within one month. The setting receiving the request must endeavour to make the changes without undue delay, on approval of the request.

12.6 The request will be recorded, along with actions and decisions undertaken in relation to the request.

12.7 The Trust / Academy has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

12.8 A child may not fully understand the risks involved in the processing of data when consent is obtained, therefore special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.9 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024
<b>Policy Owner:</b>	DPO	Page: 20 of 32			
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

12.9 Where personal data has been made public within an online environment, the Academy / Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12.10 The Trust / Academy will inform staff members involved in processing the data, where a request to erase is approved, to ensure that all data falling in the scope of the request for erasure, is erased.

### 13. The Right to Restrict Processing

13.1 Individuals have the right to restrict the Trust’s / Academy’s processing of personal data in certain circumstances. In the event that processing is restricted, the Trust / Academy will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.2 The Trust/Academy will restrict the processing of personal data in the following circumstances:

- Where the basis for processing the data is consent;
- Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy / Trust has verified the accuracy of the data;
- Where an individual has objected to the processing and the Academy / Trust is considering whether their legitimate grounds override those of the individual;
- Where processing is potentially unlawful and the individual opposes erasure and requests restriction instead;
- Where the Trust / Academy no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

13.3 If the personal data in question has been disclosed to third parties, the Trust / Academy will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.4 The Trust / Academy will inform staff members involved in processing the data, where a request to restrict processing is approved. Where a restriction on processing is subsequently lifted, staff and other third parties who process the data will be informed.

### 14. The Right to Data Portability

14.1 Individuals have the right to obtain and reuse their personal data for their own purposes and across different services.

14.2 Personal data must be moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3 The right to data portability applies:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual’s consent or for the performance of a contract
- When processing is carried out by automated means

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024
<b>Policy Owner:</b>	DPO	Page: 21 of 32			
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

14.4 Personal data will be provided in a structured, commonly used and machine-readable form.

14.5 The Trust / Academy will provide the information free of charge.

14.6 Where feasible, data will be transmitted directly to another organisation at the request of the individual. Prior to transferring the requested data, the individual must provide confirmation of their identification for the Academy / Trust. The Academy / Trust will not release the required data until after the individual's identification has been verified and that they are entitled to make the request.

14.7 SUAT and its Academies are not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8 In the event that the personal data concerns more than one individual, the Trust / Academy will consider whether providing the information would prejudice the rights of any other individual and how the data of other individuals will be adequately protected.

14.9 The Trust/Academy will respond to any requests for portability within one month.

14.10 Where the request is complex, or a number of requests have been received, the timeframe for issue can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request and will inform them of their right to complain to the supervisory authority. Requests will be responded to without undue delay.

14.11 Where no action is being taken in response to a request, the Trust/Academy will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority.

## 15. The Right to Object

15.1 The Trust / Academy will inform individuals of their right to object to their data being collected via a privacy notice, upon the point of data collection. This information will be provided clearly and explicitly.

15.2 Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest;
- Direct marketing;
- Processing for purposes of scientific or historical research and statistics.

15.3 Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation. An individual cannot exercise their right to object if they have given consent for the processing of their personal data, they must instead withdraw their consent.
- The Trust / Academy will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Trust / Academy can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 22 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

15.4 Where personal data is processed for direct marketing purposes:

- The Trust / Academy will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust / Academy cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5 Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Academy is not required to comply with an objection to the processing of the data.

15.6 Where the processing activity is outlined above, but is carried out online, the Trust / Academy will offer a method for individuals to object online.

## 16. Rights in Relation to Automated Decision Making

16.1 Article 22(1) of the UK GDPR limits the circumstances in which you can make solely automated decisions, including those based on profiling, that have a legal or similarly significant effect on individuals.

16.2 Solely means a decision-making process that is totally automated and excludes any human influence on the outcome. A process might still be considered solely automated if a human inputs the data to be processed, and then the decision-making is carried out by an automated system.

16.3 Any processing of this nature must be consulted with the DPO, prior to this being undertaken. Processing of this nature must be agreed by the DPO and the data subject must consent. A DPIA must also be undertaken.

## 17. Privacy by Design and Default

17.1 The Trust and Academies will act in accordance with the UK GDPR by adopting a privacy by design approach, and implementing technical and organisational measures which demonstrate how the Trust and Academies have considered and integrated data protection into processing activities.

17.2 Data protection impact assessments (DPIAs) will be used to assess and manage the risks involved with certain data processing activities to identify the most effective method of complying with the Academy's / Trust's data protection obligations and meeting individuals' expectations of privacy.

17.3 The aim of the DPIAs is to allow the Trust / Academy to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Academy / Trust / Data Subject which might otherwise occur. An effective DPIA will help to:

- Identify, manage and mitigate data protection risks
- Fix problems at an early stage, minimising those risks
- Consider and mitigate risks to individuals' privacy

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>				
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024	
<b>Policy Owner:</b>	DPO	Page: 23 of 32				
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>

- Ensure individuals' expectations of privacy obligations are being met - for example, by the provision of privacy notices
- Provide individuals with reassurance
- Demonstrate both accountability and compliance with data protection law
- Avoid reputational damage

17.4A DPIA will be used when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of biometric data
- The use of data relating to vulnerable individuals

17.5The Trust / Academy will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

17.6Where a DPIA indicates high risk data processing, the Trust / Academy staff will refer to the DPO who will undertake consultation with the ICO as required to seek its opinion as to whether the processing operation complies with the UK GDPR.

17.7As a DPIA is not a one-off exercise, this should be kept under regular review and updated if anything changes in the data's life cycle, for example, changes to the processing of the personal data or the amount of personal data collected. Reviews may occur when:

- A security flaw is identified
- Technology is made available
- A contractor is appointed
- Public concern is raised over the type of processing done
- Public concern is raised over the vulnerability of a particular group of data subjects

17.8The data processing activity must have a basis in law and additional conditions for data defined as SCD.

17.9Ensure that staff involved in the data processing are involved in preparing and reviewing the DPIA.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 24 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

## 18. Data breaches

18.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A data breach is a security incident that has resulted in personal data being:

- Lost or stolen
- Destroyed without consent
- Changed without consent
- Accessed by someone without permission

18.2 At Trust level the DPO / CEO / Deputy CEOs will ensure that all staff members are made aware of, and understand, what constitutes as a data breach as part of their continuous development training. At Academy level this will be the responsibility of the Principal / Head Teacher and Data Protection Lead. All members of staff must be trained to:

- Recognise when a personal data breach has taken place
- Know how to report it formally in accordance with the personal data breach management plan

18.3 Where the Trust / Academy holds concerns about an issue relating to data privacy, this must be reported to the DPO immediately, for support, advice and investigation.

18.4 Those who suspect that there may be a potential personal data breach must follow SUAT's Personal Data Breach Management Plan (located in Teams), which includes the required reporting procedures, immediately upon notification or discovery of the potential breach.

18.5 Once an individual becomes aware of a suspected data breach, a check must be made to establish whether the breach involves personal information. If personal data is involved, it must be established as to what types of personal data are involved and who the data subjects are. The investigation must identify many people are affected by the breach to help determine the level of risk involved.

Risk is the risk to the people who are affected; how seriously people might be harmed and the probability of this happening. This will consider all the information currently available, for example:

- Who's affected
- How many people are affected
- The ways it might affect them, such as:
  - Safeguarding issues
  - Identity theft
  - Significant distress



Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 25 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

18.6 The priority is to establish what has happened to the personal data; where the personal data that has been accessed, lost or stolen now is, and who might have it. If the data can be recovered, this must be done immediately and protect those who'll be most impacted.

18.7 The person reporting the breach must use the 'Potential Personal Data Breach Report Form,' provide sufficient information to allow an investigation to start and send this via email to the DPO. The DPO will ask for further information as necessary.

18.8 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed, following an initial assessment by the DPO. The DPO will make the report.

18.9 All notifiable breaches will be reported to the Information Commissioner's Office within 72 hours of the Trust/Academy becoming aware of it. The report will be made by the DPO, or the CEO/Deputy CEOs, in the absence of the DPO. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis. This must be documented accordingly.

18.10 The breach will be investigated using SUAT breach notification and investigation templates. Any actions taken in relation to managing and mitigating the breach will also be recorded. The data breach log will be completed by the Academy and Trust.

18.11 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Trust / Academy will notify those concerned directly, without undue delay and upon advice of the ICO, where necessary.

18.12 In the event that a breach is sufficiently serious, the public will be notified without undue delay, in consultation with the ICO and insurance providers.

18.13 If the breach involves a cyber incident, the Cyber Incident Response Plan will be followed. The breach will be reported to the relevant authorities which may include Action Fraud, the Police, the NCSC.

18.14 Effective and robust breach detection, investigation and internal reporting procedures are in place at the Trust and its Academies, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified. The personal data breach management plan and cyber incident plans will be updated annually. Staff will be trained and receive annual refresher training as a minimum, regarding what constitutes as a breach and how to report this.

18.15 Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 26 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.16 Failure to report a breach when required to do so can result in a fine, as well as a fine for the breach itself. Fines will be operated on a two-tier system by the ICO. The fine is dependent on factors such as the measures that were undertaken to mitigate the risk of the breach occurring, and the nature of the breach.

18.17 The ICO helpline, 0303 123 1113 can provide support in assessing the impact and taking appropriate steps, including how to let data subjects know. Data breaches can be reported via phone or online: [Report a personal data breach](#) to the Information Commissioner’s Office.

18.18 After every personal data breach or near miss, the following should be reviewed:

- What happened
- How it happened
- Why it happened
- What actions can be taken to prevent it happening again

In accordance with DfE guidance, every personal data breach shall be recorded and investigated, and trend analysis should be undertaken.

18.19 It is important to take steps to reduce the possibility of personal data breaches occurring. Prevention can include:

- Mandatory data protection training undertaken annually for all staff, that includes how to recognise and report a personal data breach
- Ensuring that staff have an awareness of common data breaches and how they can be avoided, such as by checking recipients and attachments are correct before sending emails
- Having appropriate controls in place to protect personal data

## 19. Data security

19.1 The Academies and Trust are required to adhere to the Information Security Policy.

19.2 Personal and confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.3 Personal and confidential paper records will not be left unattended or in clear view in locations with general access. Clear desk policies are required.

19.4 Staff must lock or log out of electronic devices when they are not in use, to prevent unauthorised access. Devices must be encrypted.

19.5 Passwords are not shared and are kept secure at all times, changed on a regular basis in accordance with the password section of the Information Security Policy.

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024
<b>Policy Owner:</b>	DPO	Page: 27 of 32			
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

19.6 Digital data is encrypted both locally and on back ups. Back ups will follow the NCSC's 3-2-1 back up policy.

19.7 Personal and business critical data is not saved on removable storage or a portable device. Any devices used for non critical and non personal data will be kept in a locked filing cabinet, drawer or safe when not in use. All devices of this nature must be encrypted and must be provided by the Academy or Trust, and secured appropriately by the IT Support provider.

19.8 All electronic devices must be password-protected and encrypted to protect the information on the device in case of theft and where possible, electronic devices allow the remote blocking or deletion of data in case of theft.

19.9 Staff, Trustees and Local Academy Council members will make every effort not to use their personal laptops or computers for SUAT purposes. Personal devices which are used for SUAT purposes will not be used to store or access personal or confidential information.

19.10 All members of staff are provided with their own secure login and password, and every computer must regularly prompt users to change their email password on a termly basis. Emails and MIS systems must be subject to multi factor authentication.

19.11 Emails containing sensitive or confidential and personal information should be encrypted.

19.12 Circular emails to parents or personal email accounts are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.13 Confidential or personal identifiable information must not be sent by fax; alternative secure methods for transferring data must be sought.

19.14 Where personal information that could be considered private, confidential or personally identifiable is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same security procedures (Information Security Policy). The person taking the information from the Academy premises accepts full responsibility for the security of the data.

19.15 Privacy surrounding the sharing of personal data is inclusive of verbal communications. Staff must follow the code of conduct.

19.16 Before sharing personal data, all staff members will ensure:

- They follow the Data Sharing Policy.
- They are allowed to share it.
- That adequate security is in place to protect it.
- The party receiving the data has been outlined in a privacy notice/consent form/data collection form, and the recipient is authorised to receive the data.
- 

19.17 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas containing sensitive information are supervised at all times. Visitors use guests wifi to access internet services and agree to acceptable use policies.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 28 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

19.18 Staff must remain extra vigilant when clicking on links and SharePoint requests or opening attachments which are sent via email, **no matter who they appear to come from**. Staff must not click on or enter email account information into any email links or SharePoint requests they are unsure of or are not expecting, and must check the legitimacy with the sender. If staff have any concerns surrounding email security, this must be reported to their IT provider immediately. Staff will be trained in cyber security on an annual basis.

19.19 Settings should be aware of what personal data they store within the Academy network, and what's stored outside of their direct control. Both locations must have in place good security settings, including encryption and access control, and all those processing personal data should be trained in keeping data safe. DfE has guidance to help schools [keep people and their personal data safe](#) when using digital technology, and on [meeting ICT service and equipment standards](#).

19.20 The physical security of buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place. Each Academy has a security risk assessment in place.

19.21 SUAT takes its duties under the UK GDPR seriously and unauthorised disclosure of personal information is not permitted.

19.22 Archived data must be kept secure at all times, either electronically through password protection, or through suitable locked storage facilities. The DPO should be contacted to advise regarding data continuity and resilience matters.

19.23 Decisions in relation to the processing of personal data will be recorded.

19.24 The government's National Cyber Security Centre has resources to improve cyber resilience. They include:

- [Information about better protection in cyberspace](#)
- [Device security guidance](#)
- [Cloud security principles](#)
- [Tools to strengthen cyber defence](#)
- [Cyber security training for staff](#)
- [Home learning technology advice](#)
- [Data security tips](#)

The police service's regional cyber protect officers provide free advice and training to schools.

## 20. Publication of information

20.1 SUAT publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 29 of 32			
Audience:	Trustees <input checked="" type="checkbox"/> Parents <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	

20.2 Classes of information specified in the Publication Scheme are made available in accordance with our Freedom of Information Policy and Publication Scheme.

20.3 SUAT will not publish any personal information, including photos, on its website without the consent of the affected individual, unless there is a lawful basis for publishing this information (for example, governance information must be published in accordance with the Academies Handbook).

## 21. CCTV and photography

21.1 The Trust / Academies understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. Data of this nature that is collected is done so in compliance with the CCTV Policy.

21.2 The Trust/Academy notifies all Trustees, LAC members, pupils, staff and visitors of the purpose for collecting CCTV images via appropriate means including the privacy notice, and other such measures which may include notice boards / signage, letters and email.

21.3 Cameras are placed where they do not intrude on anyone's privacy and are necessary to fulfil a specific purpose and have a basis in law for their use.

21.4 All CCTV footage will be kept for 30 days. The Academy Principal and Data Protection Lead are responsible for ensuring the records are secure and allowing access - supporting CCTV data processing compliance in accordance with the Data Protection Policy and CCTV Policy.

21.5 The Trust / Academies will use photographic / video personal data in accordance with the Use of Images Policy. Images will never be taken on personal devices.

21.6 If the Trust/Academy wishes to use images/video footage of pupils in a publication, such as websites, prospectus, or recordings of Academy plays, written permission will be sought for the particular usage from the parent of the pupil (or the student themselves, depending on their age). The pupil's wishes in relation to their data must be considered and managed.

21.7 Images captured by individuals for domestic purposes, and videos made by parents for family use, are exempt from the UK GDPR.

21.8 Those using CCTV, photography and videos should refer back to the Use of Images and CCTV Policies.

## 22. Data retention

22.1 Data will not be kept for longer than is necessary in line with the Trust's Compliant Records Management Policy / Retention Policy.

22.2 Data that reaches its retention period will be deleted / destroyed as soon as practicable, and recorded in the data destruction log. The Data Protection Act 2018 and UK GDPR says data should only be kept for as long as it is needed unless there is a legal reason to continue processing the data. All personal data must be disposed of securely.

Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	Trust Board	Issue date:	May 2023	Review date:	May 2024
Policy Owner:	DPO	Page: 30 of 32			
Audience:	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	
	Parents <input checked="" type="checkbox"/>	General Public <input checked="" type="checkbox"/>			

22.3 Some educational records relating to former pupils or employees of the Trust / Academy may be kept for an extended period for legal reasons, but also to enable the provision of references, academic transcripts, historical or archiving purposes. Data which is retained must be anonymised wherever possible, without losing its meaning.

22.4 Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained. Electronic memories are inclusive of those relating to leased devices such as photocopiers and printers.

22.5 The Academy/Trust must ensure that any copies of personal data are not retained beyond specified retention periods, inclusive of those which are held with third parties.

22.6 The Data Retention Policy will consider:

- The reasons that the data is being held
- If there's a legal duty to keep the information for a set period of time
- Whether the data is shared
- Whether it's more appropriate for another organisation such as the local authority to keep the information in the long term
- If the data is needed to meet Ofsted's requirements
- Whether the data should be deleted or depersonalised
- If there is a justification to keep the data

22.7 An audit of all the personal data each setting holds, should be undertaken each year, to check it is up to date and still needed. Data destruction logs can be shared with Trustees and LAC members to demonstrate compliance with the DPA 2018. This includes:

- Databases
- Online systems
- Paper records
- Videos and photos

Reviewing the personal data will help to identify what data needs to be:

- Kept
- Destroyed
- Changed from a paper format to an electronic format
- Kept for research or litigation purposes

22.8 The Trust uses the IRMS Toolkit for Academies to inform its set retention periods.

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024
<b>Policy Owner:</b>	DPO	Page: 31 of 32			
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

22.9As data becomes older, there are steps that can be taken to keep data about pupils for analytical purposes. Before deleting the data completely, remove names and personal identifiers. Another option is to replace the personal information with non-personal identifiers. For example, replace the:

- Name with a random ID
- Date of birth with year of birth
- Postcode with locality or town name

22.10When records have reached the end of their retention period, data must be disposed of securely and confidentially. All records containing personal information or sensitive policy information must be made either unreadable or so they cannot be reconstructed. Do not dispose of records with the regular waste or in a skip. Data can be disposed of by:

- Shredding paper records using a cross-cutting shredder, or get a compliant external company to shred them
- Destroy storage media and hard disks to particles no larger than 6mm
- Dismantle and shred audio and video tapes

External companies should:

- Shred all records on-site in the presence of an employee
- Be able to prove that the records have been destroyed and provide a certificate of destruction
- Have trained its staff in the handling of confidential documents

The Freedom of Information Act 2000 requires a list of records that have been destroyed and who authorised their destruction, to be maintained:

1. A senior leader has approved the record to be destroyed.
2. Document the destruction. Record a brief description of the data, the number of files and who authorised the destruction.
3. Shred the records as soon as they have been documented as having been destroyed.

### 23. DBS data

23.1All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS will never be duplicated.

DBS data will be collected in line with the Safer Recruitment Policy, Keeping Children Safe in Education and the Compliant Records Management Policy. Copies of DBS certificates will not be taken.

<b>Staffordshire University Academies Trust</b>		<b>Trust Policy Document</b>			
<b>Approved by:</b>	Trust Board	<b>Issue date:</b>	May 2023	<b>Review date:</b>	May 2024
<b>Policy Owner:</b>	DPO	Page: 32 of 32			
<b>Audience:</b>	Trustees <input checked="" type="checkbox"/>	Staff <input checked="" type="checkbox"/>	Pupils <input checked="" type="checkbox"/>	Local Academy Council <input checked="" type="checkbox"/>	Parents <input checked="" type="checkbox"/> General Public <input checked="" type="checkbox"/>

23.3 DBS data will remain strictly confidential and be kept secure at all times, and only be accessed by those who need the data to perform their role.

**24. Policy Review**

24.1 This policy is reviewed every year.

24.2 The policy will be reviewed by the DPO and MAT SLT.

24.3 The policy will be shared with all academies on review.

24.4 The policy will be uploaded to the website.