Staffordshire University Academies Trust		Trust Policy Document			
Approved by:	**Trust Board**	**Issue date:**	**May 2022**	**Review date:**	**May 2023**
Policy Owner:	**DPO**	Page: **1 of 18**			
Audience:	**Trustees** ☑ **Staff** ☑ **Pupils** ☑ **Local Academy Council** ☑ **Parents** ☑ **General Public** ☒				

UK GDPR – Data Protection Policy

Statement of intent
Staffordshire University Academies Trust (SUAT) is required to process information about its staff members, pupils and other stakeholders in accordance with its legal obligations under the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018), and this policy outlines SUAT's obligations under the data protection legislation. Whilst the European Union's (EU) General Data Protection Regulation (GDPR) is an EU Regulation and no longer applies to the UK, the Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period and UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK only context. The Information Commissioner's Office (ICO) continues to remain 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). It also gives data subjects various rights regarding 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 and recognises that the correct and lawful treatment of personal data is important in maintaining confidence in SUAT and in how it operates both through its business and educational functions.

This policy is applicable to all people working in SUAT (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities. Any breach of this policy may result in disciplinary action. This policy is in place to ensure all staff, 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 (GDPR)
- The Freedom of Information Act 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
Department for Education Data Protection: A Toolkit for Schools

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

- Compliant Records Management Policy

- IT Acceptable Use Policy
- Freedom of Information Policy
- CCTV Policy
- 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.

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.

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:

(a) Ensuring that all personal data is kept securely and security management measures are sufficient;
(b) 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;
(c) Ensuring that personal data is kept in accordance with the Trust's retention schedule;
(d) Ensuring that queries regarding data protection, including subject access requests and complaints, are promptly directed to the DPO as necessary;
(e) 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 resolving breaches;
(f) Where there is uncertainty around a data protection matter, advice is sought from the DPO;
(g) Providing the required training and inductions for staff or arranging this with the DPO, and ensuring that refresher training is undertaken annually;
(h) Maintaining records of training;
(i) Communicating with the DPO where a Data Protection Impact Assessment be required;
(j) Supporting data protection audits.

Staff have responsibilities to ensure:

(a) All personal data is kept securely throughout its lifespan;

(b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
(c) Personal data is kept in accordance with the Trust's retention schedule;
(d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the responsible person at each Academy;
(e) 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;
(f) Where there is uncertainty around a data protection matter advice is sought from the responsible person and DPO;
(g) Training and inductions are attended, including annual refresher training;
(h) Communicating with the responsible person where new processing activities are due to take place so that a DPIA can be considered and arranged;
(i) Supporting data protection audits.

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

(a) 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;
(b) 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;
(c) The Trust / Academies receive prior notification of any disclosure of personal data to any other organisation or any person;
(d) 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;
(e) 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, and that consent to process personal data is obtained where necessary.

2. Applicable data

2.1 For the purpose of this policy, 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, including information such as an online identifier, for example an IP address. Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available

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.

2.3 Examples of places where personal data might be found are:

- On a computer database
- In a file, such as a pupil report
- A register or contract of employment
- Pupils'/students' exercise books, coursework and mark books

- Health records
- Email correspondence
- Governance records
- Payroll data

2.4 Sensitive personal data is referred to in the GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person (e.g. fingerprints)
- Data concerning health (mental and physical health) and medical records
- Data concerning a natural person's sex life or sexual orientation
- Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences should be treated in the same way to special category data
- Information concerning child protection matters
- Special educational needs

3. Principles

3.1 In accordance with the requirements outlined in the UK GDPR, personal data will 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).
- 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).

- 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).

3.2 The UK GDPR requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". Personal identifiable information must be processed in a manner which provides accountability in compliance with the UK GDPR principles in order to demonstrate a robust process for the protection of personal identifiable information. Processing activities shall be documented effectively. (Accountability Principle).

3.3 "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing personal data. 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 their information, how long it is kept for and about their right to complain to the Information Commissioner's Office (ICO), the data protection regulator. This information is provided in the SUAT's privacy notices and can be obtained from the SUAT and Academy websites.

3.4 If Personal Data is being used in a way that does not comply with data protection law, this must be raised with the DPL or DPO.

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.

4.2 The Trust will provide comprehensive, clear and transparent template privacy notices for Academies to adapt for their setting.

4.3 Records of activities relating to higher risk processing will be maintained and supported by a Data Protection Impact Assessment.

4.4 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 personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place

4.5 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.

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

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 the Trust and its Academies 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 audits, and providing the required training to staff members.

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

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

5.6 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 will 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 the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained (or approved individual acting on their behalf provides consent).
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Examples of this within SUAT include processing personal data to ensure that:

- SUAT provides a safe and secure environment
- Pastoral care can be provided
- Education and learning for pupils/students can be provided, including additional activities for pupils/students and parents/carers (for example activity clubs)
- SUAT's interests and objectives are promoted and protected
- The welfare and wellbeing of pupils/students/staff is safeguarded and promoted
- SUAT's contractual and other legal obligations are met

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.

6.3 Special category data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by data protection laws.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of applicable laws which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

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.

7. Consent

7.1 Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

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 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.

7.5 Consent can be withdrawn by the individual at any time and 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.

7.6 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 can be determined by the child, so long as the child understands the impact(s) of providing their consent.

7.7 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 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.

7.8 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.

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

7.10 Where consent to process personal data is not redacted over time, 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.

7.11 Consent should be refreshed at regular intervals, and individuals informed regarding the procedure for withdrawing their consent, upon providing this.

8. The right to be informed

8.1 The privacy notice supplied to individuals in regard to the processing of their personal data 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.

8.2 Where the Academy is required to provide a privacy notice for a child, it will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

8.3 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- Legitimate interests of the controller.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period or criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:

— Withdraw consent at any time.
— Lodge a complaint with a supervisory authority.

- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences (Academies will not implement automated decision making without first completing a DPIA and consulting with the DPO).

8.4 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.

8.5 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.

8.6 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7 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.

9. The right of access

9.1 Individuals have the right to obtain confirmation that their data is being processed. The Trust has a Subject Access Request procedure on the website to support the management of such requests.

9.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3 The SAR must be made in writing wherever possible, however, 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.

9.4 The scope of the information which the individual wishes to access must be precise. The request must be made directly with the individual Academy/Trust and must include the name and contact details of the requester, alongside clear and accurate details of what data the individual is requesting, and the time frame to which the data relates. The Academy/Trust cannot process a SAR without a clear scope of information, and the time frame to which the data relates.

9.5 The Trust/Academy will verify the identity of the person making the request, by suitable means, before any information is supplied. Information can only be provided once the verification of the data subject's identity has been made. Following verification, the data shall be released without undue delay but within one calendar month, unless an extension is required. Where an extension is required, this will be assessed and agreed by the DPO. Up to a further two months may be agreed for responding to a complex request. 'Suitable means' will be defined at the discretion of the Academy and/or the DPO according to their knowledge and records regarding the individual.

9.6 A copy of the information will be supplied to the individual free of charge; however, the Trust / Academy may impose a 'reasonable fee' to comply with requests for further copies of the same information.

9.7 Where a SAR has been made electronically, the 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.

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

9.9 In the event that the requested personal 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.

9.10 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.

9.11 All fees will be based on the administrative cost of providing the information.

9.12 All requests will be acknowledged, and responded to without undue delay.

9.13 In the event of numerous or complex requests, the period of compliance may be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within 30 days of the receipt of the request.

9.14 Where a request is manifestly unfounded or excessive, 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 30 days of the refusal.

9.15 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.

9.16 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:

- Relevant 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 those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

- Any views the child or young person has on whether their parents 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. The right to rectification

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

10.2 The Academy/Trust must be satisfied of the identity of the individual requesting the rectification, prior to making the rectification.

10.3 Where the personal data in question has been disclosed to third parties, the Trust/ Academy will inform them of the rectification required.

10.4 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.

10.5 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. The individual will be informed of the extension and their right to complain to the supervisory authority within 30 days.

10.6 Where no action is being taken in response to a request for rectification, 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 and to a judicial remedy.

11. The right to erasure

11.1 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.

11.2 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
- The Academy/Trust must be satisfied of the identity of the individual making the request, prior to erasing personal data.

11.3 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

11.4 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.

11.5 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.

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

12. The right to restrict processing

12.1 Individuals have the right to block or suppress the Trust's/Academy's processing of personal data in certain circumstances.

12.2 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.

12.3 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 has verified the accuracy of the data;
- Where an individual has objected to the processing and the Academy 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.

12.4 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.

12.5 The Trust/Academy will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

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

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

13.3 The right to data portability only applies in the following cases:

- 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

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

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

13.6 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.

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

13.8 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.

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

13.10 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.

13.11 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 and to a judicial remedy.

14. The right to object

14.1 The Trust/Academy will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2 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.

14.3 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.

14.4 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.

14.5 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.

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

15. Rights in relation to automated decision making

15.1 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.

15.2 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.

15.3 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.

16. Privacy by design and privacy impact assessments

16.1 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.

16.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Academy's/Trust's data protection obligations and meeting individuals' expectations of privacy.

16.3 DPIAs will 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's/Trust's reputation which might otherwise occur.

16.4 A 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.

16.5 A DPIA will be used for more than one project, where necessary.

16.6 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

16.7 The 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

16.8 Where a DPIA indicates high risk data processing, the Trust / Academy 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. Data breaches

16.1 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.

16.2 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.

16.3 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.

16.4 Those who suspect that there may be a potential personal data breach must follow SUAT's Personal Data Breach Management Plan (located on the website) which includes the required reporting procedures, immediately upon notification or discovery of the potential breach. The person reporting the breach will use the 'Potential Personal Data Breach Report Form.'

16.5 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

16.6 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.

16.7 The breach will be investigated using SUAT breach notification and investigation templates to record such actions.

16.8 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.

16.9 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.

16.10 In the event that a breach is sufficiently serious, the public will be notified without undue delay.

16.11 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.

16.12 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
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

16.13 Failure to report a breach when required to do so will 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 what measures were undertaken to mitigate the risk of the breach occurring, and the nature of the breach.

18. Data security

18.1 The Academies and Trust adhere to the Information Security Policy.

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

18.3 Personal and confidential paper records will not be left unattended or in clear view anywhere with general access. A 'clear desk policy' is in place.

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

18.5 Passwords are not shared and are kept secure at all times.

18.6 Digital data is encrypted both on a local hard drive and on a network drive that is regularly backed up off-site.

18.7 Where personal data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. All devices of this nature must be encrypted.

18.8 Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

18.9 All electronic devices are password-protected and encrypted to protect the information on the device in case of theft.

18.10 Where possible, the Academy enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.11 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 personal or confidential information.

18.12 All members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their email password on a termly basis.

18.13 Emails containing sensitive or confidential and personal information are encrypted.

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

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

18.16 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 procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Academy premises accepts full responsibility for the security of the data.

18.17 Privacy surrounding the sharing of personal data is inclusive of verbal communications.

18.18 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.
- Who will receive the data has been outlined in a privacy notice, and the recipient is authorised to receive the data.

18.19 Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas containing sensitive information are supervised at all times.

18.20 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 to 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.

18.21 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.

18.22 SUAT takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.23 The Data Protection Officer is responsible for supporting continuity and recovery measures to ensure the security of protected data.

18.24 Archived data must be kept secure at all times, either electronically through password protection, or through suitable locked storage facilities.

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

19. Publication of information

19.1 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

19.2 Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3 SUAT will not publish any personal information, including photos, on its website without the consent of the affected individual.

19.4 When uploading information to the Trust or Academy website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. CCTV and photography

20.1 The Trust/Academy understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

20.2 The Trust/Academy notifies all Trustees, LAC members, pupils, staff and visitors of the purpose for collecting CCTV images via the privacy notice, notice boards, letters and email.

20.3 Cameras are placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

20.4 All CCTV footage will be kept for 30 days for security purposes; 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.

20.5 The Trust/Academy will always indicate its intentions for taking photographs of pupils and will ensure written permission before publishing them.

20.6 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. The pupil's wishes in relation to their data are also accounted for.

20.7 Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

20.8 Refer back to the Use of Images and CCTV Policies.

21. Data retention

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

21.2 Unrequired data/data that is beyond its retention period will be deleted / destroyed as soon as practicable.

21.3 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.

21.4 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.

21.5 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. DBS data

22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

22.2. Data provided by the DBS will never be duplicated.

22.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

22.4. DBS data will be collected in line with the Safer Recruitment Policy, Keeping Children Safe in Education and the Compliant Records Management Policy.

22.5. DBS data will remain strictly confidential and be kept secure at all times.

23. Policy review

1.1 This policy is reviewed every year by the Chief Operating Officer and the Data Protection Officer.

22.2 The next scheduled review date for this policy is May 2023.