Thinking Schools Academy Trust
"Transforming Life Chances"

Data Protection Policy

This policy was adopted on	December 2019
The policy is to be reviewed on	December 2021

1. Policy Statement

1.1 Everyone has rights with regard to how their personal information about them is handled. During the course of our activities we will collect, store and otherwise process personal information about our pupils, pupils' families, staff, volunteers, contractors, suppliers, and other third parties.

1.2 Thinking Schools Academy Trust are committed to meeting their legal obligations concerning data protection and confidentiality and to seeking to achieve best practice in relation to information governance.

1.3 Any breach of this or any other information governance policy will be taken seriously and may result in legal action being taken against the Academy, the Trust and/or the individual responsible for the breach.

2. Definitions

2.1 "*The Trust*" means Thinking Schools Academy Trust.

2.2 *"Data"* means Personal Data and Special Category Personal Data.

2.3 *"Data Controller"* is the person who or the organisation which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. "*Data Subject*" means all living individuals about whom the Academy holds Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in respect of their Data and the information that the Academy holds about them.

2.4 *"Data Processor*" means any person who or organisation which processes Data on behalf of the Data Controller including contractors, and suppliers and any third party whose work involves accessing or otherwise using Data held by the Academy. Data Processors have a duty to protect the information they process for and on behalf of the Academy by following this and other Academy information governance policies at all times.

2.5 "*Data Protection Legislation*" means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.6 "*Personal Data*" means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.7 "*Processing*" means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

destruction. Processing also includes transferring personal data to third parties. "*Special Category Personal Data*" means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.

2.8 "*Social Media"* means websites and applications that enable users to create and share content or to participate in social networking including Facebook, LinkedIn, Twitter, Google+, and all other social networking sites, internet postings and blogs. It applies to use of Social Media for Academy purposes as well as personal use that may affect the Academy in any way.

2.9 "*Subject Access Request*" ("SAR") means a request by an individual to the Trust or the Academy pursuant to Article 15 of the GDPR.

3. Data Protection Officer

3.1 The Trust and its Academies are required to appoint a Data Protection Officer ("DPO").

3.2 The DPO for the Trust is Mr Lee Miller who can be contacted on privacy@tsatrust.org.uk.

3.3 The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this and other information governance policies. Any questions about the operation of this or any other information governance policies should be referred in the first instance to the DPO.

3.4 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

4. Data Protection Principles

4.1 Anyone Processing Data must comply with the data protection principles. These provide that Data must be:

i. Processed fairly and lawfully and in a transparent manner in relation to the data subject;
ii. Collected for specified, lawful purposes and not further processed in a way which is not incompatible with those purposes;
iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
iv. Accurate and, where necessary, kept up to date;
v. Not kept in an identifiable form for longer than is necessary for the purpose; and
vi. Processed securely using appropriate technical and organisational measures.

4.2 Personal data must also be processed in accordance with data subjects' rights, and not transferred to people or organisations situated in other countries without adequate protection.

4.3 We will comply with the data protection principles and the rights of Data Subjects in the Processing of any Data.

5. Conditions for Processing Personal Data

5.1 Personal Data can only be processed if at least one of the conditions for Processing in the Data Protection Legislation applies. We will normally Process Data based on the following conditions:

5.1.1 Where the Processing is necessary for the performance of a contract between us and the Data Subject, such as an employment contract;

5.1.2 Where the Processing is necessary to comply with a legal obligation that we are subject to;

5.1.3 Where the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of our functions as set down by law; and

5.1.4 Where none of the above apply then we will usually seek the consent of the Data Subject to the Processing of their Data.

6. Conditions for Processing Special Category Personal Data

6.1 Special Category Personal Data can only be processed where an additional condition for Processing applies. We will normally only Process Special Category Personal Data based on the following conditions:

6.1.1 Where the Processing is necessary for the purpose of carrying out our obligations or exercising our rights in relation to employment law, for example in relation to sickness absence;

6.1.2 Where the Processing is necessary for reasons of substantial public interest based on either national or EU law, for example for the purposes of equality of opportunity and treatment;

6.1.3 Where the Processing is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and

6.1.4 Where none of the above apply then we will usually seek the consent of the Data Subject to the Processing of their Special Category Personal Data.

Vital Interests

6.1.5 There may be circumstances where it is considered necessary to Process Data in order to protect the vital interests of a Data Subject. This might include medical emergencies where the Data Subject is not in a position to give consent to the Processing. We believe that this will only occur in very specific and limited circumstances. In such circumstances, we would usually seek to consult

with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

6.1.6 Where none of the other bases for Processing set out above applies then we must seek the consent of the Data Subject before processing any Data for any purpose.

6.1.7 There are strict legal requirements in relation to the form of consent that must be obtained from Data Subjects.

6.1.8 In relation to pupils in School Year 7 and below, we will seek consent from an individual with parental responsibility for that pupil.

6.1.9 We will generally seek consent directly from a pupil who is in School Year 8 and above, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.

6.1.10 If consent is required, then this form of consent will:

6.1.10.1 Inform the Data Subject of exactly what we intend to do with their Data;

6.1.10.2 Require them to positively confirm that they consent; and

6.1.10.3 Inform the Data Subject of how they can withdraw their consent.

6.1.11 Any consent must be freely given, and we will not make the provision of any goods or services or other matter conditional on a Data Subject giving their consent.

6.1.12 The DPO must always be consulted in relation to any consent form before consent is obtained.

6.1.13 A record must be kept of any consent, including how it was obtained and when.

7. Rights of Data Subjects

7.1 Data will be processed in line with Data Subjects' rights.

7.2 Data Subject have a right to be informed about:

7.2.1 Our identity and contact details as Data Controller and those of the DPO;

7.2.2 The purpose or purposes and legal basis for which we intend to Process their Data;

7.2.3 The types of third parties, if any, with which we will share or to which we will disclose their Data;

7.2.4 Whether the Data will be transferred outside the European Economic Area and if so the safeguards in place;

7.2.5 The period for which their Data will be stored;

7.2.6 The existence of any automated decision making in the Processing of their Data along with the significance and envisaged consequences of the Processing and the right to object to such decision making; and

7.2.7 The rights of the Data Subject to object to or limit Processing, request information, request deletion of information or lodge a complaint with the ICO.

7.3 Data Subjects also have a right to:

i. Request access to any Data held about them by a Data Controller (for further detail see our Subject Access Request Policy);
ii. Object to the Processing of their Data, including the right to object to direct marketing;
iii. Have inaccurate or incomplete Data about them rectified;
iv. Restrict Processing of their Data;
v. Have Data we hold about them erased;
vi. Have their Data transferred; and
vii. Object to the making of decisions about them by automated means.

8. Data Security

8.1 We will ensure that appropriate security measures are taken against unlawful or unauthorised Processing of Data, and against the accidental loss of, or damage to, Data.

8.2 The Data Protection Legislation requires that we put in place procedures and technologies to maintain the security of all Data from the point of collection to the point of destruction.

8.3 Data may only be transferred to a third party Data Processor if they agree to comply with those procedures and policies, or if they otherwise put in place adequate measures to our satisfaction. We will always ensure that a contract is in place with any Data Processor, which is compliant with Data Protection Legislation.

8.4 For further information on the types of data processors, that information may be passed to please refer to our Privacy notice on the Trust and Academy websites.

8.5 For further information and details of the applicable security measures, please see the Information Security policy.

9. Disclosure and sharing of Information

9.1 We may share Data we hold with another school, the Trust, the Local Authority, the Department of Education, Ofsted, statutory bodies, health professionals and examination bodies or any other body where we have a lawful basis for doing so.

9.2 Anyone who receives enquiries from third parties should be careful about disclosing any Data that we hold. In particular they must:

i. Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;

ii. Require that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;

iii. Refer to the DPO for assistance in difficult or unusual situations; and

iv. Where providing information to a third party, do so in accordance with the data protection principles and the provisions of this Policy.

10.0 Processing of Images

10.1 Parents and others attending Academy & Trust events are allowed to take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Trust does not prohibit this as a matter of policy.

10.2 The Trust does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Trust to prevent.

10.3The Trust asks that parents and others do not post any images or videos, which include any child other than their own child on any social media or otherwise publish those images or videos.

10.4 As an Academy & Trust, we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

10.5 Whenever a pupil begins their attendance at the Academy, they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

11 CCTV

11.1 The Trust operates a CCTV system. Please refer to the Trust CCTV Policy.

12 Biometric Recognition Systems

12.1 Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash we will comply with the requirements of the Protection of Freedoms Act 2012.

12.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

12.3 Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

12.4 Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

12.5 As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

12.6 Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

13. Monitoring and Review

13.1 This policy will be reviewed every 2 years or earlier if required and may be subject to change.

APPENDIX 1

Data Protection Impact Assessment

Data Protection Impact Assessment (DPIA) for new Projects or Systems

General Details

Project Title	
Project Lead	
Contact Details	
DPO	
Contact Details	
Date DPIA Completed	

General Project Description
Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties:

Will the project/system involve the processing of personal data or special category (sensitive) personal data?

YES / NO

If '**No**', please sign and forward the DPIA to the IT Security Manager, Head of Programme Office and Director of IT for their awareness and stored by the DPO for accountability purposes.

If '**Yes**', please complete the sections below:

1. Systematic Description of the Envisaged Processing Operations

1.1 Create a Data Flow Diagram and attach it as Annex 1 to this DPIA.

1.2 Identify the data subjects:

1.3 What personal data will be processed?

1.4 What special category (sensitive) data or criminal convictions data will be processed?

1.5 What are the purposes and lawful grounds for processing the personal data identified above?

	Personal Data	Purpose	Lawful basis
1			
2			
3			
4			
5			

1.6 Describe the nature, scope and context of the processing, including a functional description of the processing operations:

1.7 Describe the assets on which the personal data relies (hardware, software, people, paper, networks, transmission channels)

1.8 Set out the periods for retention of the personal data:

1.9 Set out details of any data sharing with third parties, including sub-processors:

1.10 Set out details of any data sharing outside the EEA or with any international organisations:

2. Necessity and Proportionality Assessment

2.1 If legitimate interest is identified as the lawful basis, set out details below:

a) Identify the legitimate interest

b) Explain why processing is necessary for the identified legitimate interest

c) Balance the legitimate interest against the rights and freedoms of the data subjects

2.2 Identify any personal data processed in a manner which is not necessary for the identified purpose:

3. Assessment of Risks to the Rights and Freedoms of the Data Subjects

Consider and describe the risks to the rights and freedoms of the data subjects in the following areas:

3.1 Lawfulness of processing

3.2 Fairness and transparency of processing

3.3 Data minimisation

3.4 Maintaining accurate and up to date data

3.5 Ability for data subjects to opt out or object to processing

3.6 Ability to respond to subject access requests

3.7 Rights of the data subjects

3.8 Transfers to third parties

3.9 Transfers outside the EEA or to international organisations

3.10 Retention and deletion

3.11 Data security

3.12 Further risks

4. Measures Envisaged to Address the Risks

4.1 Complete the following table using the risks identified above:

	Risk	Controls to be implemented	Proposed Mitigation
1			
2			
3			
4			
5			

5. Compliance with Guidance/Codes of Conduct

5.1 Identify any applicable guidance and/or codes of conduct issued by the Government, the ICO, the Commission or any relevant association or body:

5.2 Where applicable, set out details of compliance with any relevant guidance and/or code of conduct:

6. Involvement of Data Subjects

6.1 Where appropriate, seek the views of the data subjects or their representatives on the intended processing and set out the findings below:

6.2 If the views of the data subjects have not been sought, set out the rationale below, with reference to any commercial or public interests and the security of processing operations:

7. DPIA Review

7.1 Identify any planned changes to the project or system and set a date to review this DPIA:

8. Approval

This project was assessed, and its Data Protection Impact Assessment approved:

Headteacher Name…….

Headteacher Signature…….

Headteacher Date: ……...

Data Protection Officer Name: ……

Data Protection Officer Signature……

Data Protection Officer Date……

Action	Completed
Privacy Notice updated	
Consent obtained from data subjects	
Updated DATA Mapping Spreadsheet	
Other:	
Other:	

Annex 1 – Data Flow Diagram