Thinking Schools Academy Trust
“Transforming Life Chances”

Data Protection Policy

This policy was adopted on	June 2021
The policy is to be reviewed on	June 2023
This policy is ratified by the Governance & Compliance Committee	

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 and its trading subsidiaries

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

2.3 *"Data Controller"* is the organisation which determines 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 UK-General Data Protection Regulation (UKGDPR) 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 UK-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 The Trust will comply with the data protection principles and the rights of Data Subjects in the Processing of any Data.

5. Age Appropriate Design Notice Principles

5.1 The Trust complies with the Age Appropriate Design Code (also known as The Children's Code) and the fifteen principles enshrined within it:

1. Best Interests of the child
2. DPIA
3. Age Appropriate application
4. Transparency
5. Detrimental use of Data
6. Policies and community standards
7. Default Settings
8. Data Minimisation
9. Data Sharing
10. Geolocation
11. Parental Controls
12. Profiling
13. Nudge Techniques
14. Connected Toys & Devices
15. Online tools

6. Conditions for Processing Personal Data

6.1 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 on the basis of the following conditions:

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

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

6.1.3 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;

6.1.4 Where the Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data

subject which require protection of personal data, in particular where the subject is a child;

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

7. Conditions for Processing Special Category Personal Data

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

7.1.1 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;

7.1.2 Where the Processing is necessary for reasons of substantial public interest on the basis of UK law, for example for the purposes of equality of opportunity and treatment;

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

7.1.4 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

7.1.5 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

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

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

7.1.8 In relation to pupils in School Year 8 and below we will seek consent from an individual with parental responsibility for that pupil.

7.1.9 We will generally seek consent directly from a pupil who is in School Year 9 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.

7.1.10 If consent is required then this form of consent will:

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

7.1.10.2 Require them to positively confirm that they consent; and

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

7.1.11 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.

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

8. Rights of Data Subjects

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

8.2 Data Subject have a right to be informed about:

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

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

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

8.2.4 Whether the Data will be transferred outside the UK and if so the safeguards in place;

8.2.5 The period for which their Data will be stored;

8.2.6 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

8.2.7 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.

8.3 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.

9. Data Security

9.1 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.

9.2 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.

9.3 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 appropriate measures are in place with any Data Processor which is complaint with Data Protection Legislation.

9.4 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.

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

10. Sharing of Data

10.1 We may share data we hold with other data controllers or data processors where we have a lawful basis for doing so.

10.2 We will share data with our suppliers or contractors to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

a) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

b) Only share data that the supplier or contractor needs to carry out their service

c) Only share data where we have a legal basis to do so

10.3 For any new data processor appointed a Data Protection Impact Assessment (DPIA) will be completed to assess the processors compliance. Staff should contact the DPO for advice on completing a DPIA

10.4 We will share data with other agencies where we have a legal basis to do so, this includes child protection data in line with our legal obligations to keep children safe. Further information on the Trusts legal duties regarding the sharing of child protection data can be found within the Trust Safeguarding Policy.

10.5 Where we transfer personal data internationally, we will do so in accordance with data protection law.

10.6 Where a new processor or system is a website, application or online service being used by children within our trust the DPIA will assess their compliance against the age appropriate design code

10.7 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

v. Only share with organisations on the approved data processors and data controllers list. If the requester is not listed on there, a DPIA must be completed

11. Processing of Images

11.1 As part of our regular activities we may take images and recording of individuals.

11.2 As an Academy and 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, or their

parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

11.3 Consent can be withdrawn at any point. If consent is withdrawn the images will be deleted and not distributed further.

12. CCTV

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

13. Biometric Recognition Systems

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

13.2 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.

13.3 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.

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

13.5 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).

13.6 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.

14. Monitoring and Review

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