



LANGTREE SCHOOL

DATA PROTECTION POLICY

LANGTREE SCHOOL ACADEMY TRUST COMPANY
AN EXEMPT CHARITY LIMITED BY GUARANTEE
COMPANY NUMBER 7980335

In this policy as in all documents of The Langtree School Academy Trust Company ("TLSATC") any reference to Langtree School, School, Governors of Langtree School or Trustees of Langtree School Academy Trust Company is a reference to The Board of Directors of The Langtree School Academy Trust Company and any reference to the Headteacher of Langtree School is a reference to the Chief Executive Officer of TLSATC.

STATUS:			
RECOMMENDED		STATUTORY	✓
REVIEW FREQUENCY		Annual	
DATE OF POLICY		June 2025	
DATE OF LAST REVIEW		June 2026	
REVIEW DUE		June 2027	
EXECUTIVE LEAD		Business Manager	
COMMITTEE		Finance & General Purposes	
Signed: Chair of Trustees			

Contents

1. Aims	2
2. Legislation and Guidance	3
3. Definitions	3
4. The Data Controller	4
5. Data Protection Principles	4
6. Roles and responsibilities	4
7. Privacy/Fair Processing Notice	5
7.1 Students and parents	5
7.2 Staff	5
7.3 Trustees	6
8. Subject Access Requests	6
9. Parental Requests to see the Educational Record	7
10. Data Accuracy	7
11. CCTV	8
12. Biometric recognition systems	8
13. Authorized Use of Integrated AI Tools (Google Workspace)	9
13.1 Scope and Approval	9
13.2 Prohibited Tools	9
13.3 Data Input Restrictions	9
13.4 Human Oversight and Accountability	9
13.5 Lawful Basis for Processing	9
13.6 Compliance and Risk Management	9
14. Storage of records	9
15. Disposal of Records	10
16. Training	10
17. Monitoring Arrangements	10
18. Links with other policies	10
19. Contact	11

1. Aims

Our School aims to ensure that all data collected about staff, students, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR).

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of Data Protection Legislation, and is based on:

- [guidance published by the Information Commissioner's Office](#) and
- [model privacy notices published by the Department for Education](#);
- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Data Protection Act 2018 \(DPA 2018\)](#).

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and guidance from the Department for Education (DfE) on [Generative artificial intelligence in education](#).

This policy also covers requirements of [Keeping Children Safe in Education 2023 \(KCSIE 2023\) paragraphs 141 and 142 Filtering and Monitoring](#).

It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.

It also reflects the ICO's [guidance](#) for the use of surveillance cameras and personal information.

In addition, this policy also complies with other Academy Funding Agreements and Articles of Association.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation

	• Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording, storing, altering or destruction of data
Data subject	The living individual whose personal data is held or processed
Data controller	A person or organisation that determines the purpose for which, and the way in which personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The Data Controller

Our School processes personal information relating to students, staff, parents, students' emergency contacts and visitors, and therefore is a data controller.

The School / Trust is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data Protection Principles

The UK GDPR is based on the following data protection principles, or rules for good data handling.

Data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.
- collected 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.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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.
- 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.

6. Roles and Responsibilities

The Trustees have overall responsibility for ensuring that the School complies with its obligations under the UK GDPR.

Day-to-day responsibilities rest with the Headteacher. The Headteacher will ensure that all staff are aware of their data protection obligations, and will oversee any queries related to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the School of any changes to their personal data, such as a change of address.

Data breach reporting is mandatory under the UK GDPR and all staff are made aware of their obligation to report data breaches without delay.

7. Privacy/Fair Processing Notice

7.1 Students and Parents

We hold personal data about students to support teaching and learning, to provide pastoral care and to assess how the School is performing. We may also receive data about students from other organisations including, but not limited to, other schools, Local Authorities, the Department for Education and the National Health Service.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on student characteristics, such as ethnic group or Special Educational Needs and Disabilities
- Exclusion information
- Details of any medical conditions.

We will retain the data we collect only for as long as is necessary to satisfy the purpose for which it was collected.

We will not share information about students with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this Policy.

Once our students reach the age of 13, we are legally required to pass on certain information to the youth support services provider in our area, which has responsibilities in relation to the education or training of 13 - 19 year-olds. Parents, or students aged 16 or over, can request that only their name, address and date of birth be passed to this agency by informing the School Business Manager.

We are required by law to pass certain information about students to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our School / Trust. The purpose of processing this data is to assist in the running of the School, including to:

- enable individuals to be paid
- facilitate safer recruitment practice
- support the effective performance management of staff
- improve the management of workforce data across the education sector
- inform our recruitment and retention processes
- allow better financial modelling and planning
- enable monitoring of people with, and without, protected characteristics under the Equality Act
- support the work of the School Teachers' Review Body.

Staff personal data includes, but is not limited to, information such as:

- contact details, next of kin
- National Insurance numbers
- salary information
- qualifications
- absence data
- personal characteristics/protected characteristics
- medical information
- outcomes of any disciplinary procedures.

We will retain the data we collect only for as long as is necessary to satisfy the purpose for which it was collected.

We will not share information about staff with third parties without consent unless the law allows us to. This may include advisers such as our Occupational Health and our Human Resources advisers.

We are required by law to pass certain information about staff to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

Any staff member wishing to see a copy of the information about them that the school holds should contact the Headteacher.

7.3 Trustees

We process data relating to Trustees of the School. The purpose of processing this data is to assist in the running of the School, including to:

- ensure that all Trustees have valid DBS checks carried out
- maintain up to date records at the Local Authority, the Department for Education and Companies House.

Trustee personal data includes, but is not limited to, information such as:

- contact details
- date of birth
- term of office dates
- business interests
- biography information for the School website.

We will retain the data we collect only for as long as is necessary to satisfy the purpose for which it was collected.

We will not share information about Trustees with third parties without consent, unless the law allows us to. We are required by law to pass certain information about Trustees to specified external bodies, such as the Local Authority, the Department for Education and Companies House, so that they can meet their statutory obligations.

Any Trustee wishing to see a copy of information about them that the School holds should contact the Headteacher.

8. Subject Access Requests

Under the UK GDPR, Staff, Students and Parents/Carers have a right to request access to information the School holds about them. This is known as a Subject Access Request (SAR).

Subject Access Requests must be submitted in writing, either by letter or email. Requests should include:

- The subject's name
- A correspondence address
- A contact number and email address
- Details about the information requested.

Before a Subject Access Request is processed, the identity of the requestor will be verified by the School to ensure information is released only to the correct person.

The Trust will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that a child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child.

Subject Access Requests for all or part of the student's educational record will be provided within 15 school days of receiving the request.

If a Subject Access Request does not relate to the educational record, we will respond within one calendar month.

We reserve the right to charge for requests that are deemed to be excessive.

9. Parental Requests to see the Educational Record

Parents of students at this School do not have an automatic right to access their child's educational record. The School will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

For a parent to make a Subject Access Request, the child must either be unable to understand their rights and the implications of a Subject Access Request or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents of students at our School may not be granted without the express permission of the student.

If parents ask for copies of information, they will be required to pay the cost of making the copies.

10. Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the School of a change of circumstances, his/her computer records will be updated as soon as is practicable.

Data Checking Sheets for students will be provided to data subjects so they can check its accuracy and make any amendments as follows:

- On entry to Year 7
- On transfer to Year 10

Data Checking Sheets will be issued to staff every 12 months .

Where a data subject challenges the accuracy of his/her data the school will immediately mark the record as potentially inaccurate, or "challenged". In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes should be referred to the Board of Trustees under the formal Complaints Procedure.

11. CCTV

We use CCTV in various locations around the School site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are

being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the School Business Manager.

12. Biometric Recognition Systems

Note that in the context of the Protection of Freedoms Act 2012, a “child” means a person under the age of 18.

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.

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 obtain written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school’s biometric system(s). We will then provide alternative means of accessing the relevant services for those pupils. For example, pupils can access the cashless system in the canteen using a PIN number.

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

As required by law, if a pupil refuses to participate in, or to 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).

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. Authorized Use of Integrated AI Tools (Google Workspace)

13.1 Scope and Approval

The School recognizes that integrated AI tools within the **Google Workspace for Education** environment can enhance administrative efficiency, support drafting and summarization, and improve accessibility. Staff are permitted to use these approved tools provided they use **school-provided accounts**, which are configured to ensure that organizational data and prompts are not used to train Google’s general large language models, and that processing remains within the langtreeschool.com domain.

13.2 Prohibited Tools

The use of **consumer-grade AI tools** (such as public ChatGPT or personal Gemini accounts) for the processing of any School-related personal or sensitive data remains **strictly prohibited**. Entering personal or sensitive data into unauthorized generative AI tools will be treated as a data breach.

13.3 Data Input Restrictions

Staff must adhere to the following restrictions when inputting data into authorized AI tools:

- **Special Category Data:** Staff are explicitly prohibited from inputting special category data (e.g. health information, ethnicity, or sensitive safeguarding details) into AI tools unless it is strictly necessary and a specific **Data Protection Impact Assessment (DPIA)** has been conducted and approved.
- **Anonymisation:** Whenever possible, staff should use anonymised data to avoid the unnecessary exposure of personally identifiable information.

13.4 Human Oversight and Accountability

AI should assist, not replace, human decision-making.

- **Human Review:** Staff must critically evaluate and fact-check all AI-generated outputs before sharing or publishing them. Reliance on AI outputs without human review is prohibited.
- **Automated Decision-Making:** The use of AI for **automated decision-making** that could have legal or similarly significant effects on students or families is strictly forbidden.
- **Transparency:** Any documents, presentations, or formal communications influenced by AI should be clearly labelled to indicate AI assistance.

13.5 Lawful Basis for Processing

The School processes data using these integrated AI tools under the lawful basis of **Public Task (Article 6(1)(e))**, as the tools are used to support core educational and administrative functions.

13.6 Compliance and Risk Management

A robust **Data Protection Impact Assessment (DPIA)** must be maintained for the Google Workspace AI suite, covering the types of data entered, risks of bias or inaccuracy, and necessary staff training. Improper use of AI tools or failure to adhere to these standards will be subject to disciplinary action.

14. Storage of records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are to be kept under lock and key when not in use.
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the School office. Staff must adhere to School policies and procedures when taking data off site.
- Passwords that are at least 8 characters long containing letters and numbers are used to access School computers, online resources, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices. Encryption, anonymisation and pseudonymisation are used to protect the data.
- Staff, students or Trustees who store personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment.
- Trustees are required to use school email addresses and use cloud storage for sharing information and data.
- UK GDPR compliant cloud storage will be used for all online data storage.

15. Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely according to the School / Trust Data Destruction Policy.

For example, we will shred or incinerate paper-based records, and override electronic files. We also use an outside company to convert paper records to electronic and to shred documents on site.

16. Training

Our staff and Trustees are provided with data protection training as part of their induction process, and this is refreshed annually each September.

Data protection also forms part of continuing professional development, where changes to legislation or the School's processes make it necessary to keep staff up to date.

17. Monitoring Arrangements

The Headteacher is responsible for monitoring and reviewing this policy.

The School Data Protection Officer checks that the school complies with this policy by, among other things, reviewing school records at least annually or more frequently if required.

This policy will be reviewed annually by the Board of Trustees.

18. Links with Other Policies

This Data Protection Policy is linked to:

- The Remote Working Policy
- The Freedom of Information Publication Scheme
- Privacy Notice (Student and Parent)
- Privacy Notice (Staff Workforce)
- Records Management Policy
- Use of Email Policy
- Data Destruction Policy
- Record Retention Policy
- CCTV Policy

19. Contact

If you would like to discuss anything in this privacy, In the first instance please contact the School Lead below:

Position	Name	Email	Phone
School Lead	Business Manager	cventress@langtreeschool.com	01491 220131
Data Protection Officer	Turn It On	<u>dpo@turniton.co.uk</u>	01865 597620 (option 3 GDPR)

Policy Update Information (policy number GDPR-101)

This policy is reviewed annually and updated in line with data protection legislation.

Policy review information

Review date	Reviewed by
02-05-2018	turn IT on
08-08-2019	turn IT on
01-08-2020	turn IT on
02-08-2021	turn IT on
04-08-2022	turn IT on
01-08-2023	turn IT on

Policy update information

Review date	Revision	Description of change	By
02-05-2018	1.00	Draft release	turn IT on
03-05-2018	1.00	Full release	turn IT on
08-08-2019	1.01	Full release	turn IT on
08-08-2019	1.02	Full release	turn IT on
01-08-2020	1.03	Full release	turn IT on
02-08-2021	1.04	Full release	turn IT on
01-08-2023	1.05	Full release	turn IT on

Appendix A: DPIA Template: Use of Sensitive Data in Authorised AI Tools

1. Project Overview & Data Identification	
Lead Staff Member [Insert Name/Role]	
AI Tool being used <i>(Must be a school-provided Google Workspace account)</i>	
Specific Purpose <i>(Describe why the AI tool is being used)</i>	
Sensitive Data Categories (Tick all that apply)	☐ Physical or Mental Health Information ☐ Racial or Ethnic Origin ☐ Safeguarding / Child Protection Details ☐ Special Educational Needs (SEN) Information ☐ Other (please add details)
2. Necessity and Proportionality	
Strict Necessity <i>(Explain why this task cannot be completed using anonymised data or traditional methods)</i>	
Data Minimisation <i>(Confirm input has been limited to the absolute minimum amount of sensitive data required)</i>	
3. AI-Specific Risk Assessment	
Accuracy (Hallucination Risk) <i>(How will you ensure the AI has not 'hallucinated' or altered facts?)</i>	
Bias and Discrimination <i>(Is there a risk the AI might produce biased summaries?)</i>	
Over-reliance <i>(What steps are in place to ensure a human is making the final decision?)</i>	
4. Security and Safeguarding Protocols	
Contractual Assurance <i>(Confirm you are using a School account)</i>	

where data is not used to train Google's general models)	
Access Control (Who will have access to the AI-generated output?)	
Safeguarding (Does this use of AI align with KCSIE protocols?)	
5. Mitigation and Human Oversight	
Mandatory Human Review (Describe your process for fact-checking the output)	
Labelling (Confirm the final document will be clearly marked as 'AI-Assisted')	
Automated Decision-Making (Confirm this AI tool is not being used to make an automated decision with legal or significant effects)	
6. Sign-off and Approval (Applicant Section)	
Staff Member Declaration (I confirm I have received AI-specific data protection training and will remain professionally accountable for the output.)	Applicant Signature Date
DPO Review	DPO Comments and Risk Level Statement
Headteacher/CEO Approval	Signature Date:

Note: The lawful basis for processing this data is stated as **Public Task (Article 6(1)(e))** and **Substantial Public Interest (Article 9)**.¹