Full name of policy:	**Data Protection Policy**		
Name and post of person responsible:	Nathan Hatch (Data Protection Officer)		
Frequency of review:	Annually		
Dates of previous reviews:	Sept 22, Sept 23, Oct 2024		
Date of next formal review:	Sept 26		
Policy Reference:	All policies can be located on the "Information for staff" Team Drive		
Total number of pages: (Including appendices and front sheet)	10		
Comments:			
	Name (role):	**Signature:**	**Date:**
Written:	Nathan Hatch (Data Protection Officer)	N Hatch	01/09/21
Ratified:	Jan Balon - Headteacher	J Balon	03/09/21
Reviewed:	Nathan Hatch (Data Protection Officer)	N Hatch	20/03/26
Ratified:	Jan Balon - Headteacher	J Balon	11.5.26

Contents

London Academy of Excellence Tottenham is committed to actively promoting equality of opportunity in everything that it does and to ensuring that differences between all of our learners and staff are valued and respected. This policy complies with the 2010 Equality Act.

This Data Protection Policy will be reviewed annually.

1. Aims

London Academy of Excellence Tottenham ("LAET" or "the School") is committed to ensuring that all personal data relating to students, staff, parents/carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

This policy applies to all personal data processed by the School, whether held electronically or in paper format.

The School aims to:

- Comply fully with UK data protection legislation
- Protect the rights and freedoms of individuals
- Maintain high standards of information security and confidentiality
- Promote transparency and accountability in data handling
- Ensure staff understand their responsibilities when handling personal data

2. Legislation and Guidance

This policy complies with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- Protection of Freedoms Act 2012 (where applicable)
- ICO guidance for schools and educational settings
- Department for Education (DfE) guidance, including Generative Artificial Intelligence in Education

3. Definitions

Personal data

Information relating to an identified or identifiable living individual.

Special category data

More sensitive personal data requiring additional protection, including health information, ethnicity, religion and biometric identifiers.

Processing

Any operation performed on personal data including collection, storage, use, sharing or deletion.

Data subject

The individual to whom the data relates.

Data controller

The organisation determining how and why personal data is processed. LAET is the data controller.

Data processor

A third party processing data on behalf of the School.

Personal data breach

A breach of security leading to accidental or unlawful loss, disclosure, alteration or access to personal data.

4. The Data Controller

London Academy of Excellence Tottenham is registered with the Information Commissioner's Office (ICO) and pays the required data protection fee.
The School acts as the data controller for personal data processed in carrying out its educational and operational functions.

5. Roles and Responsibilities

5.1. Governing Body

The Governing Body has overall responsibility for ensuring compliance with data protection legislation.
It will:

- Approve this policy
- Monitor compliance
- Ensure adequate resources are available for data protection

5.2. Data Protection Officer (DPO)

The DPO:

- Oversees compliance with data protection law
- Advises on data protection impact assessments (DPIAs)
- Acts as contact point for the ICO
- Monitors policy implementation
- Provides advice to staff and leadership

DPO: Nathan Hatch
Contact: dpo@laetottenham.ac.uk
The DPO operates independently and reports directly to senior leadership and governors.

5.3. Headteacher

The Headteacher acts as the operational representative of the data controller and ensures day-to-day compliance.

5.4. All Staff

All staff must:

- Process personal data lawfully and securely
- Follow School policies and procedures
- Report suspected data breaches immediately
- Complete required training
- Only access data necessary for their role
- Ensure that they inform the school of any changes to their own personal data

Failure to comply may result in disciplinary action.

6. Data Protection Principles

The School complies with UK GDPR principles. Personal data must be:

1. Processed lawfully, fairly and transparently
2. Collected for specified legitimate purposes
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up to date
5. Retained only as long as necessary

6. Processed securely
7. Accountable and demonstrably compliant

7. Collecting personal data

7.1. Lawfulness, fairness and transparency

The School processes personal data where one or more lawful bases apply:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual has freely given clear consent

For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

7.2. Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it,

we will inform the individuals concerned before we do so, and seek consent where necessary.
Staff must only process personal data where it is necessary in order to do their jobs.
We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.
In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule

8. Sharing Personal Data

Personal data may be shared where lawful and necessary, including with:

- Department for Education
- Local authorities
- Examination bodies
- Safeguarding partners
- IT service providers
- Law enforcement agencies

The School will:

- Use data sharing agreements where required
- Share only minimum necessary information
- Ensure third parties provide adequate safeguards

International transfers will comply with UK GDPR requirements.

9. Subject access requests and other rights of individuals

9.1. Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address

- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

9.2. Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. In the case of a parental request for data, the School will normally provide access where lawful and appropriate. Students aged 16+ will normally exercise their own access rights unless consent is given otherwise.

9.3. Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4. Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain

circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Educational Records - Parental Requests

As an academy, there is no automatic statutory parental right of access to educational records; however, the School will normally provide access where lawful and appropriate.
Students aged 16+ will normally exercise their own access rights unless consent is given otherwise.

11. CCTV

The School operates CCTV systems to maintain safety and security.
The School will:
- Display clear signage
- Use CCTV proportionately
- Retain recordings only as long as necessary
- Restrict access to authorised personnel only

CCTV use complies with ICO surveillance camera guidance.
Enquiries regarding CCTV should be directed to the DPO.

12. Photographs and Videos

The School may take photographs or videos for educational, promotional or communication purposes.
Consent will be obtained from:
- Students aged 18+, or
- Parents/carers where required.

Images will not be used alongside unnecessary identifying information.
Consent may be withdrawn at any time.

13. Artificial Intelligence (AI)

AI tools present both educational opportunities and data protection risks.
The School requires that:
- Personal or sensitive data must not be entered into unauthorised AI systems.
- Staff must follow School guidance when using generative AI tools.
- Any inappropriate disclosure via AI tools will be treated as a data breach.

Please see the school's AI Policy for further details.

14. Data Protection by Design and Default

The School embeds data protection into all activities by:

- Completing DPIAs for high-risk processing
- Limiting data collection
- Maintaining records of processing activities
- Reviewing systems regularly
- Training staff appropriately

15. Data Security and Storage

The School will protect personal data through:

- Secure passwords and access controls
- Encryption of portable devices
- Locked storage for paper records
- Secure transfer methods
- Restricted user permissions

Personal data must not be stored on personal devices unless authorised.

16. Retention and Disposal

Records are retained in accordance with the **DfE Records Management Toolkit for Schools**.

Data will be securely deleted, shredded or destroyed when no longer required.

17. Personal Data Breaches

All suspected breaches must be reported immediately to the DPO.

The School will:

- Investigate breaches promptly
- Mitigate risks
- Maintain breach records
- Notify the ICO within 72 hours where required
- Inform affected individuals where risk is high

18. Training

All staff and governors receive:

- Data protection training during induction
- Regular refresher training
- Updates where legislation or risks change

Training records are maintained.

19. Monitoring and Review

The DPO will monitor compliance and review this policy annually.

The Governing Body will approve all revisions.

20. Related Policies

This policy links to:

- LAET N075 - Safeguarding and promoting the welfare of children
- LAET N040 - ICT Acceptable Use Policy

- LAET N042 - Freedom of Information publication scheme
- LAET N043, LAET N044, LAET N052 and LAET N054 - Privacy Notices
- Records Retention Schedule