[Add school logo and name]

part of the

LDBS Academies Trust

LAT and LAT 2

Data Protection Policy

Document type	School Policy	Statutory DfE / Trust	DfE
Approval Level	Trust Board of Directors	Review Frequency	Annual
Approval date	21/05/2026	Next Review Date	20/05/2027
On behalf of the Trust Board of Directors			
Name	Andrew Garwood-Watkins	Name	Christalla Jamil
Position	Chair of the Board of Trustees of the Trusts	Position	CEO of the Trusts
On behalf of Choose an item.			
Name		Name	
Position	Chair of the School Board of Governors	Position	Headteacher
Publication to	☒ GovHub	☐ Staff info site	☒ Website

NOTE TO THE LOCAL ACADEMY COMMITTEES – MAY BE DELETED UPON LAC ADOPTION

This is the Data Protection Policy template. A space is foreseen above for the school to add its own name and logo. A box below is foreseen for the school to add its school-specific Values. Annex 1 should be completed by the school with the school-specific information. Please do not change the formatting of titles etc as the Policy contains cross-references. This document sets minimum compliance requirements for all LDBS Academies Trust (LAT and LAT 2) schools. Each Local Academy Committee (LAC) is requested to: (i) Approve this template (with Annex 1 - School-specific details) completed; (ii) Ensure local implementation complies with this template.

Version control update log: This version updates the name of our Data Protection Officer reflects Data (Use and Access) Act 2025 requirements, including ARoP terminology, recognised legitimate interests, AI guidance, complaints electronic form, and addition of Cookies/PECR section. PLEASE

UPDATE THE TABLE OF CONTENTS FOLLOWING THE REMOVAL OF THIS SECTION (Go stand on the table of contents and you will see an “update this table” button on the top right)!

TRUST VISION STATEMENT

“The kingdom of heaven is like a mustard seed, which a man took and planted in his field. Though it is the smallest of all seeds, yet when it grows, it is the largest of garden plants and becomes a tree, so that the birds come and perch in its branches.” (Matthew 13: 31-32)

In the parable of The Mustard Seed, Jesus reminds us that even the smallest of seeds has the potential to grow into the fullness of itself. We aim to provide the right environment for our children, and all whom we serve, to flourish into the fullness of themselves. He tells us these seeds grow into trees, capable of providing a home for a rich diversity of life, our work is to ensure all in our communities grow into people of compassion and wisdom with a deep spiritual understanding of how to support the needs of others.

SCHOOL VISION

Click or tap here to enter text.

Table of Contents

LIST OF ANNEXES

1 Aims

The LDBS Academies Trust (LAT and LAT 2, hereafter collectively referred to as "the Trust") and its schools aim to ensure that all personal data collected, stored, processed and destroyed about any natural person, whether they be a member of the school workforce, pupil/student, parent, Director, Local Academy Committee member, visitors, contractor, consultant, or any other individual is done so in accordance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018), Data (Use and Access) Act (DUAA) 2025 and the Privacy & Electronic Communications (EC Directive) Regulations (PECR) 2011.

This policy applies to all personal data processed by the school, regardless of whether it is in paper or electronic format, or the type of filing system it is stored in, and whether the collection or processing of data was, or is, in any way automated.

2 Legislation and guidance

This policy meets the current requirements of UK Data Protection legislation. It is based on guidance published by the Information Commissioner's Office (ICO) on the EU GDPR, PECR 2011, UK GDPR, DUAA 2025 and DPA 2018. It is also based on the information provided by the Article 29 Working Party.

Additionally, it meets the requirements of the Protection of Freedoms Act 2012, ICO's code of practice in relation to video surveillance, and the DBS Code of Practice in relation to handling sensitive information. Furthermore, this policy complies with the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3 Definitions

Term	Definition
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, following the Controller's instruction.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Consent	Freely given, specific, informed and unambiguous indication of the data subject's wishes via a statement or by a clear affirmative action, signifying agreement to a specific processing of personal data relating to them.
Personal data	Any information relating to an identified or identifiable natural person ('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.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including Information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation • History of offences, convictions or cautions (*) (*) Note: Whilst criminal offences are not listed as special category data, within this policy they are regarded as such in acknowledgment of the extra care which is needed with this data set.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal 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 can be automated or manual.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4 The Data Controller

Both the LDBS Academies Trust (No. ZA089623) and the LDBS Academies Trust 2 (No. ZA229902) (hereafter collectively referred to as "the Trust") are registered as a data controllers with the Information Commissioner's Office (ICO) and will renew this registration as legally required. The Trust collects and determines the processing for personal data relating to parents/carers, pupils, the school workforce, governors/volunteers, visitors and others. The Trust moreover processes data on the behalf of others and is therefore considered both a data controller and a data processor.

5 Roles and responsibilities

This policy applies to all individuals employed by our Trust, to all the schools that are part of the Trust, and to external organisations or individuals working on our behalf. Employees who do not comply with this policy may face disciplinary action.

5.1 Board of Directors

The Trust Board of Directors has overall responsibility for ensuring that the Trust and all the Trust schools comply with all relevant data protection obligations. The Trust will seek to perform its responsibility by reviewing this policy regularly, appointing a Data Protection Officer (DPO) and delegating the responsibility to implement this policy to the Local Academy Committees (LACs).

5.2 Local Academy Committees (LACs)

The LACs have delegated responsibility to review this policy's implementation at the school level. Every LAC has a link member for Data Protection. The name of this school's link member can be found in Annex I.

5.3 Data Protection Officer (DPO)

The Trust has appointed Grow Education Partners Ltd as its Data Protection Officer (DPO). The responsible contact for the LDBS Academies Trust is Jay Makwana (jay.makwana@london.anglican.org or 020 3837 5073) and for the LDBS Academies Trust it is David Coy, (david.coy@london.anglican.org or via mobile on 07903 50653).

They are responsible for overseeing the implementation of this policy, along with any future development of this or related policies/guidelines and reviewing our compliance with data protection law.

Upon request the DPO can provide an annual report of the Trust or school's compliance status directly to the Board of Directors or LAC and provide their advice and recommendations on Trust / school data protection issues.

The DPO is a named point of contact for the ICO and all Data Subjects whose data the school processes.

Full details of the DPO's responsibilities are set out in GROW Education Partner's Service Level Agreement with the Trust.

5.4 The Headteacher

Each Headteacher acts as the representative of the Data Controller on a day-to-day basis.

5.5 All Employees

Employees (regardless of role) are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, e.g., a change of address, telephone number, or bank details.
- Reporting a Data Breach, Data Rights Request, or Freedom of Information Request.

- Contacting the Data Protection Lead or DPO:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not, they have a lawful basis to use personal data in a particular way.
    - If they need to rely on or capture consent, draft a privacy notice/notification, or transfer personal data outside the United Kingdom.
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6 The Data protection principles

Data Protection is based on seven principles that the school must comply with. These are that personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

The Accountability principle ties these all together by requiring an organisation to take responsibility for complying with the other six principles. Including having appropriate measures and records in place to be able to demonstrate compliance.

This policy sets out how the school aims to comply with these key principles.

7 Processing personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of six 'lawful basis's (legal reasons) to do so under data protection law:

- The individual (or their parent/carer when appropriate) has freely given clear consent
- 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 e.g. 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, and carry out its official functions

- The data needs to be processed for the legitimate interests of the school or a third party, provided the individual's rights and freedoms are not overridden. [Note that Under the Data (Use and Access) Act 2025, certain processing activities, including fraud prevention, network and information security, and safeguarding, are recognised as 'recognised legitimate interests' and do not require a full balancing test to be carried out before processing can commence.]
- For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in data protection law.

These are where:

- The individual (or their parent/carer, where appropriate) has given explicit consent;
- It is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment of a Data Controller or of a Data Subject.
- It is necessary to protect the vital interests of the Data Subject;
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.
- The Personal Data has manifestly been made public by the Data Subject;
- There is the establishment, exercise or defence of a legal claim;
- There are reasons of public interest in the area of public health;
- Processing is necessary for the purposes of preventative or occupational medicine (e.g. for the assessment of the working capacity of the employee, the medical diagnosis, the provision of health or social care or treatment);
- There are archiving purposes in the public interest;

Where we collect personal data directly from individuals, we will provide them with the relevant information required by data protection law, in the form of a privacy notice.

These privacy notices can be found on the Trust's website: https://www.ldbsact.org/Policies/. The Trust has the following Privacy Notices:

- Pupils and Parents/Carers
- School Workforce (includes Trainees, Contractors and Consultants)
- Governors & Volunteers
- Job Applicants
- Visitors

Paper copies of the notices are available from the Trust's central team by calling 020 3931 8425.

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 via our privacy notices.

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.

Employees must only access and process personal data where it is necessary to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

When personal data is no longer required, employees must ensure it is destroyed. This will be done in accordance with the school data retention policy, which states how long particular documents should be kept, and how they should be destroyed.

Copies of the Data Retention Policy can be obtained by contacting the central team on info@latmat.org.uk.

8 Biometric recognition systems

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.

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.

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.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or 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 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).

9 Sharing personal data

To efficiently, effectively and legally function as a data controller we are required to share information with appropriate third parties, including but not limited to situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies or services – we may seek consent when appropriate before doing this where possible.
- Our suppliers or contractors need data to enable us to provide services to our employees and pupils (e.g. IT companies). When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law and have satisfactory security measures in place.

- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies when required to do so, these include but are not limited to:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or employees.

10 Artificial intelligence (AI)

Artificial Intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. The school recognises that AI has many uses to help pupils learn but also poses risks to sensitive and personal data. To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots. If personal and/or sensitive data is entered into an unauthorised generative AI tool. The school will treat this as a data breach and will follow the personal data breach procedure outlined in this policy.

Where AI tools are used in any form that may influence, support, or inform decisions about individuals (even where a human remains the final decision-maker), staff must ensure appropriate oversight is maintained and that such use is documented. Any AI-assisted decision-making that significantly affects a data subject must be recorded and reviewed to ensure it does not constitute automated decision-making under Article 22 of UK GDPR. Staff should contact the DPO for guidance before deploying any AI tool in contexts involving individual assessments.

11 Transferring Data Internationally

We may send your information to other countries where:

- we or a company we work with store information on computer servers based overseas; or
- we communicate with you when you are overseas.

We conduct due diligence on the companies we share data with and note whether they process data in the UK, EEA (which means the European Union, Liechtenstein, Norway and Iceland) or outside of the EEA.

The UK and countries in the EEA are obliged to adhere to the requirements of the GDPR and have equivalent legislation which confer the same level of protection to your personal data.

For organisations who process data outside the UK and EEA we will assess the circumstances of how this occurs and ensure there is no undue risk.

Additionally, we will assess if there are adequate legal provisions in place to transfer data outside of the UK.

12 Individuals Data Protection Rights

12.1 Access Rights

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

If you make a subject access request, and if we do hold information about you, we can:

- Give you a description of it.
- Tell you why we are holding and processing it, and how long we will keep it for.
- Explain where we got it from, if not from you.
- Tell you who it has been, or will be, shared with.
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this.
- NOT provide information where it compromises the privacy of others.
- Give you a copy of the information in an intelligible form.

12.2 Other Rights regarding your Data

A data subject may also

- Withdraw their consent to processing at any time, this only relates to tasks which the school relies on consent to process the data.
- Ask us to rectify, erase or restrict processing of your personal data, or object to the processing of it in certain circumstances and where sufficient supporting evidence is supplied
- Prevent the use of your personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest, official authority or legitimate interests.
- Request a copy of agreements under which your personal data is transferred outside of the United Kingdom.
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Request a cease to any processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Refer a complaint to the ICO

- Ask for your personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

The school will comply with the Data Protection legislation in regard to dealing with all data requests submitted in any format, individuals are asked to preferably submit their request in written format to assist with comprehension.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the request

If you would like to exercise any of the rights or requests listed above, please contact the representative of the Data Controller in your school (see Annex I)

If an individual receives a request, they must immediately forward it to the representative of the Data Controller (see Annex I)

We reserve the right to verify the requesters identification by asking for Photo ID, if this proves insufficient then further ID may be required.

In most cases, we will respond to requests within 1 month, as required under data protection legislation. However, we are able to extend this period by up to 2 months for complex requests or exceptional circumstances.

If the request is manifestly unfounded or excessive, we may refuse to act on it or charge a reasonable fee, which would only take into account administrative costs.

A request will be deemed to be manifestly unfounded or excessive if it is repetitive or asks for further copies of the same information.

When responding to requests, we will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual; or
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests; or
- Is contained in adoption or parental order records; or
- Is given to a court in proceedings concerning the child

In the event we refuse a request, we will tell the individual why and tell them they have the right to refer a complaint to the ICO.

Article 22 of the UK GDPR has additional rules to protect individuals from decisions made solely for the purpose of automated decision-making and profiling. The school does not carry out any automated decision-making and/or profiling on individuals.

12.3 Children and Data Rights/Requests

An individual's data belongs to them therefore a child's data belongs to that child, and not the child's parents or carers.

However, children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of invoking a data request. Therefore, for children under the age of 12 most data requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Where a child is judged to be of sufficient age and maturity to exercise their rights and a request is invoked on their behalf, we would require them to give consent to authorise the action to be undertaken.

13 Parental requests to see the educational record

Academies are not required to provide educational records if a parent requests it, as the Education (student information) Regulations 2005, which places this obligation on maintained schools, does not apply to academies. The schools of the Trust will aim to respond to a parent's reasonable request, but it should be noted that parents no longer have a legal right to this information.

Nevertheless, the Independent School Standards Regulations, which applies to academies by virtue of their funding agreement, states that the standard about provision of information is met if the Academy Trust ensures that an annual written report of each registered student's progress and attainment in the main subject areas taught, is sent to the parents of that registered student.

Requests should be made in writing to the school's contact for educational record requests (see Annex I) and should include:

- Name of individual making the request and child who the education record belongs to
- Requesters correspondence address
- Requesters contact number and email address

If an Education Record Request is received as well as a Subject Access Request and the items requested overlap, the school will determine which legislation is best suited to respond to them. We will inform the requester of the approach as part of the acknowledgment process.

14 Close Circuit Television (CCTV)

We use CCTV in various locations around the school sites and premises of the Trust for the detection and prevention of crime. However, footage may be used for additional reasons specified more fully in the CCTV Policy. We adhere to the ICO's code of practice for the use of video surveillance and provide training to staff in its use.

We do not need to ask individuals' permission to use CCTV, but in most instances we make it clear where individuals are being recorded, with security cameras that are clearly visible and accompanied by prominent

signs explaining that CCTV is in use, and where it is not clear, directions will be given on how further information can be sought.

A link to the school's full CCTV policy is provided in Annex I and a template is provided in Annex II. Any enquiries about the CCTV system should be directed to the school responsible, also specified in Annex I.

15 Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

The use of school photographs includes but is not limited to:

- Within school on notice boards and in school magazines, brochures, newsletters and prospectuses.
- Outside of school by external agencies and partners such as the school photographer, local and national newspapers and local and national campaigns we are involved with
- Online on our website or social media pages

We will obtain consent from the responsible individuals to use pupil images. When doing so we will clearly explain how the photograph and/or video will be collected and used to both the parent/carer and pupil when obtaining consent.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

You can withdraw consent by the method of withdrawal described in Annex I.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos. A link to our school Child Protection and Safeguarding Policy is provided in Annex I.

16 Cookies and the Privacy and Electronic Communications Regulations (PECR)

The Trust's websites use cookies. Cookies are small files placed on users' devices that help the website function effectively. We comply with PECR 2011 in our use of cookies.

Strictly necessary cookies (e.g. those required for the website to function) do not require user consent and are placed automatically.

Analytics and functional cookies that are low-risk may be placed without prior consent under the Data (Use and Access) Act 2025, provided clear information and an opt-out mechanism are offered to users.

Marketing or tracking cookies require explicit prior consent before being placed on a user's device.

Each school's website displays a cookie notice explaining which cookies are in use and how users can manage their preferences. Users can withdraw consent to non-essential cookies at any time via the cookie settings on the website.

Non-compliance with PECR carries fines of up to £17.5 million or 4% of global annual turnover, whichever is higher. Staff responsible for managing school websites should contact the DPO before adding any new third-party tools, plugins, or analytics services.

17 Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data collection and processing activities. These include, but are not limited to the following organisational and technical measures:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection regulations.
- Completing data privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies or processing tools. Advice and guidance will be sought from the DPO.
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Periodic audits will be undertaken to monitor and review our privacy measures and make sure we are compliant.
- Maintaining Appropriate Records of Processing (ARoP) in accordance with the Data (Use and Access) Act 2025, which replaces the previous obligation to maintain a Record of Processing Activities (RoPA) for all processing. ARoP records are required where processing presents a high risk to individuals' rights and freedoms. This includes:
    - For the benefit of data subjects, making available the name and contact details of our school DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold; maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

18 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

Our organisational and technical measures include, but are not limited to:

- Paper-based records and portable electronic devices, such as laptops, tablets and hard drives that contain personal data will be kept under lock and key when not in use. We endorse a clear desk policy.
- Papers containing confidential personal data will not be left out on display when not in use unless there is a compelling lawful basis to do so e.g. Public Task to display Allergy information in the Medical Room.

- Passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Those who utilise school-controlled devices or platforms are reminded to change their passwords at regular intervals.
- Encryption software is used to protect any devices such as Laptops, Tablets and USB Devices where saving to the hard drive is enabled.
- Employees, Pupils, Directors, LAC members or Volunteers are not allowed to store personal data on their personal devices in line with the Trust's and School's Acceptable ICT Use Agreement.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

19 Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will be rectified or updated, unless it is no longer of use and therefore will be disposed of securely.

For example, we will shred paper-based records and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law and provide a certificate of destruction.

When records are disposed of as part of the Data Retention schedule this is then recorded on our record of destruction log.

20 Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In this school, all potential or confirmed Data Breach incidents should be reported to the school's data controller representative (see Annex I), wo will assign a unique refence number to the incident and record it in the school's data breach log.

Once logged, incidents will then be investigated, the potential impact assessed, and appropriate remedial action undertaken. The DPO will be consulted as required.

Where appropriate, we will report the data breach to the ICO and affected Data Subjects within 72 hours.

The full procedure is set out in the School Data Breach Response Process, which can be found in Annex 3.

Examples of a Data Protection Breach include but are not limited to:

- Personal data being let unattended in a meeting room/in the staffroom/in the PPA room.
- Sending information relating to a pupil or family to the wrong member of staff in school, or to the wrong parent
- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils

21 Training

All employees and governors are provided with data protection training as part of their induction process.

Periodic refresher will be provided to adhere to ICO best practice or to respond to changes in legislation, guidance or the school's processes. Records of attendance will be kept ensuring that all data handlers receive appropriate training.

22 Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy as part of the general monitoring and compliance work, they carry out. They will work with School Data Protection Lead and the Lead LAC member for Data Protection (see Annex I) to ensure that this policy remains contemporaneous and appropriate for schools.

This policy will be reviewed yearly, and changes recommended when appropriate. The Trust Board of Directors will be asked to sign off the policy review and any necessary changes.

23 Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance via the school's online complaints form, by email or in writing to the school office (see Annex I). Complaints will be acknowledged within 30 days.

This complaint may be assessed by our independent Data Protection Officer:

LDBS Academy Trust Schools : Jay Makwana (jay.makwana@london.anglican.org or 020 3837 5073)

with a final response provided within 30 days.

If you are unhappy with the school's final response you can refer the matter to the Information Commissioner's Office:

Report a concern online at https://ico.org.uk/concerns/

Call 0303 123 1113

Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

24 Links with other policies

This data protection policy is linked to our:

- Freedom of information Policy
- Online Safety Policy
- Acceptable ICT User Policy

- Data Retention Schedule
- Disaster Recovery/Business Continuity Planning and Risk Register.
- Child Protection and Safeguarding Policy

Annex I - School-specific information related to this policy

The School's Data Controller Representative (a.k.a. School Data Protection Lead) is:

[Name]

[Email]

[Phone]

[Address]

The School's Local Academy Committee Link Member for Data Protection is : [name]

School contact details for Educational Record requests:

[name and contact details]

Complaints handling:

Complaints can be sent to the school via the school online complaints form location: [link to the school's online complaints form]m email to [INSERT EMAIL], or in writing to the school office. [As required by the Data (Use and Access) Act 2025, an electronic means of submitting complaints is available – school to remove this in final version].

Location of the school's CCTV Policy (see template in Annex II): [location / link]

Person responsible for the school's CCTV, who can answer questions regarding the school's CCTV system is: [name & contact details]

Pictures and Videos: [School method that parents / carers should use to withdraw their consent]

Locations of the school's:

- Safeguarding and Child Protection Policy: […]
- Acceptable ICT Use Policy […]

Annex II – School Template CCTV Policy

1. Data Protection:

Any personal data processed in the delivery of this policy will be processed in accordance with the school Data Protection Policy. Further information can also be found in the Appropriate Record of Processing (ARoP).

2. Policy Statement

[Insert school name] uses Closed Circuit Television ("CCTV") within the school site. The purpose of this policy is to set out the operation, use, storage and disclosure of CCTV at the School.

This policy applies to all data subjects whose image may be captured by the CCTV system. It works in concurrence with the School's Data Protection Policy, Record of Processing Activity and Data Retention Schedule.

The policy considers applicable legislation and guidance, including but not limited to:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act (DPA) 2018
- Video Surveillance Code of practice as produced by the Information Commissioner's Office (ICO)
- Protection of Freedom Act (PoFA) 2012
- Human Rights Act 1998.

The CCTV system is owned and operated by the school/Name of external company who supplies the system. The deployment is determined by the Senior Leadership Team, with input from the Board of Governors and Data Protection Officer (DPO).

The school will:

- Notify the ICO of its use of CCTV as part of its registration.
- Complete a Data Privacy Impact Assessment if amendments are to be made to the deployment or use of CCTV.
- Treat the system and all information processed on the CCTV system as data which is processed under DPA 2018/UK GDPR.
- Not direct cameras outside of school grounds onto private property, an individual, their property or a specific group of individuals. The exception to this would be if authorisation was obtained for Direct Surveillance as set up by the Regulatory of Investigatory Powers Act 2000.
- Display warning signs clearly in prominent places.
  Specifically, at all entrances to the school site and premises where CCTV is in use. Additionally, any public areas, where a passer-by may be recorded. Where necessary these signs will include information on how to contact the school regarding information or access to the CCTV footage.
- Not use CCTV footage for any commercial purposes.
  There is no guarantee that this system will or can cover and detect every single incident taking place in the areas of coverage.

3. Camera Setup

The CCTV system is comprised of X cameras which record day and night covering the Internal/External/Internal&External areas of the School. Their coverage also extends past the school boundaries to public areas.

Cameras will be placed so they only capture images relevant for the purposes for which they are installed, and all care will be taken to ensure that reasonable privacy expectations are not violated.

CCTV is not sited in classrooms except in exceptional circumstances.

Members of staff can request details of CCTV camera locations. The decision to provide this information will be determined by Senior Leadership and recorded as appropriate.

4. Purpose of CCTV

The School uses CCTV for the following purposes:

- To provide a safe and secure environment for the school workforce, pupils and visitors.
- To protect the school buildings and assets.
- To assist in the investigation of incidents.
- To assist in the prevention and detection of criminal activity.
- To assist law enforcement agencies in apprehending suspected offenders.

5. Covert Monitoring

The school retains the right in exceptional circumstances to set up covert monitoring. For example:

- Where there is good cause to suspect illegal or serious unauthorised action(s) are taking place, or where there are grounds to suspect serious misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from the Head Teacher and Chair of the Local Academy Committee.

Covert monitoring will cease following the completion of any investigation.

6. Storage and Retention

Recorded data will not be retained for longer than is necessary. While retained the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of people who images have been recorded.

All data will be stored securely.

CCTV footage will be kept between 7 to 30 days, unless there is a specific purpose for which they are required, then they will be retained for a longer period.

In ths school these will be stored in/on XXXX. [INSERT DETAILS OF THE SCHOOL'S DATA BACKUP PRACTICES.]

7. Access to CCTV Images

The ability to view live and historical CCTV footage is only to be provided at designated locations and by authorised persons.

Specific live monitoring is limited to SLT members, the school business manager or front office staff.

Direct access to recorded footage is limited to SLT members or the school business manager (if not part of SLT)

Only in exceptional circumstances will any other individuals be allowed to view footage. The reasons for and details of these circumstances will be recorded at the time such a decision is made.

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the school.

8. Disclosure of Images to Data Subjects (Subject Access Requests)

Any individual recorded in any CCTV image is considered a data subject and therefore has the right to request access to those images.

These requests will be considered a Subject Access Request and should follow the school's Subject Access Request process as provided in the school's Data Protection Policy.

When such a request is made, the footage will be reviewed in accordance with the request.

If the footage contains only the data subject making the request, then the individual may be permitted to view the footage.

This will be strictly limited to the footage of the data subject making the request and the specific reason for the request.

If the footage contains images of other data subjects, then the school will consider whether.

- The request requires the disclosure of the images of data subjects other than the requester, and whether these additional data subjects can be anonymized in the footage.
- The other individuals in the footage have consented to the disclosure of the images or if their consent could be obtained.
- If not, then whether it is reasonable in the circumstances to disclose those images to the data subject making the request.

The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other data subjects or jeopardise an ongoing investigation.

9. Disclosure of Images to Third Parties

The School will only disclose recorded CCTV footage to third parties where there is a lawful basis to do so.

Third parties acting on behalf of a data subject will be handled in accordance with the usual Subject Access Request process.

CCTV footage will only be disclosed to law enforcement agencies in line with the purpose for which the CCTV system is in place.

If a request is received from a law enforcement agency for the disclosure of footage, then the school will ask for an explanation of the reasoning for wanting to obtain the footage.

This will give help enable proper consideration of the extent of what can appropriately be disclosed.

If an order is granted by a court for the disclosure of CCTV images, then this will be complied with, but consideration will be given to exactly what the order requires.

In all instances, if there are any concerns as to what should or should not be disclosed then the Data Protection Officer will be contacted and further legal advice sought if necessary.

10. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance via way to raise a complaint.

This complaint may be assessed by our independent Data Protection Officer (see the Data Protection Policy for contact details), with a final response provided within 30 days.

If you are unhappy with the school's final response you can refer the matter to the Information Commissioner's Office:

Report a concern online at https://ico.org.uk/concerns/
Call 0303 123 1113
Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Annex III – Data Breach Response Process

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

Breach Notification

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify School's Data Controller Representative (see Annex I)

They will make a decision whether to refer the matter to the Data Protection Officer (DPO) (see Data Protection Policy for contact details)

Irrespective of whether the DPO is notified or not the response to the breach will follow the same path and be broken down into four distinct sections:

1. Investigation
2. Recovery
3. Reporting
4. Remedial Action

Investigation, Recovery and Reporting must be undertaken within 72hrs of breach realization. Remedial Action must be considered and decided on within this time frame but does not need to be fully enacted. 72hrs is the period of time which Data Protection Act 2018 allows for referral to the ICO or Data subjects.

Stage 1: Investigation:

All suspected breaches will be entered onto the "Data Breach Log" and assigned a unique reference number. All subsequent information will then be recorded on this log.

In addition, where required a corresponding file should be opened named after the unique reference number. All articles relating to the investigation, recovery and reporting should be stored within this file.

The first stages of the investigation into the breach report is to determine whether a breach has occurred by deciding if personal data has been accidentally or unlawfully mishandled. This will be done by assessing whether the data has been:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorized people

If a breach has been confirmed, then the severity of it will be assessed by considering:

- Data subject affected (vulnerability)
- Number of Data subjects affected.
- Data type lost, personal identifying/ special category,
- Specific Data Sets lost
- Number of Data sets
- Format of Data, electronic/paper.

Stage 2 Recovery:

The next stage is to contain and minimize the impact of the breach, this will be assisted by relevant staff members or data processors where necessary.

This may include but not be limited to:

- Contacting parties who may have received the data.
- Email Recovery
- Backup file restoration
- Requesting deletion of data.

If the data has been sent to the wrong individual and it has been requested to be deleted, confirmation of deletion should be attained in a written format for posterity.

The success or failure of the recovery must be recorded and will inform the reporting stage.

Stage 3: Remedial Action.

Once the details of the breach are known and as the recovery process is being undertaken an assessment needs to be made on what potential future action could be considered to prevent a similar breach reoccurring.

This will involve reviewing the processes and procedures which may have failed resulting in the breach.

Potential remedial actions may include, but are not limited to:

- Anonymizing and minimizing data
- Encrypted drives
- Secure access servers
- Strong password setting
- Training and support for staff and governors
- Encrypted email

All potential remedial action is to be recorded on the Data Log.

Stage 4 Reporting:

The investigator must decide who should be informed about the breach, affected data subjects and/or the ICO.

For Cyber Security or Fraud related breaches a referral to Action Fraud or National Cyber Security Centre may also be warranted.

Depending on the result of the containment efforts, the investigator will review the potential consequences, assess their seriousness and likelihood then make a decision about who needs to be informed. This will be partly determined by assessing if the risk of damage caused by the breach exceeds that of the damage that may be caused to the relationship through being informed.

If the risk of personal damage exceeds that of relationship, the Data Subjects will be promptly informed, in writing, all individuals whose personal data has been breached. This notification will set out:

A description, in clear and plain language, of the nature of the personal data breach

- The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The decision on whether to contact individuals will be documented.

A decision also needs to be made if the breach has reached the threshold to be reported to the ICO. This must be judged on a case-by-case basis.

To decide, the investigator will consider whether the breach poses a significantly risk to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:

Loss of control over their data

- Discrimination
- Identify theft or fraud
- Financial loss
- Unauthorized reversal of pseudonymization (for example, key-coding)
- Damage to reputation
- Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The decision will be documented either way, in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored *Place Decisions are documented*

Where the ICO must be notified, this will be done via the 'report a breach' page of the ICO website, or through their breach report line (0303 123 1113), within 72 hours. As required, the reporter will set out all known details of the breach including recovery attempts and their success. Potential remedial action will be included if known.

If all the breach details are not yet known, then as much as is known should be reported to the ICO within 72 hours. The report will explain that there is a delay, the reasons why, and when the further information is expected to be known. Then the remaining information will be submitted as soon as possible

At the conclusion of all stages of the Data Breach a mini report can be supplied to the Headteacher and Local Academy Committee to brief them the outcome and propose ways it can be prevented from occurring again.

This is to allow the school's Local Academy Committee to hold the school accountable as per the Accountability Principle.