Data Protection Policy

This policy is effective throughout the Learning without Limits Academy Trust including both the Central Team and each of its Academies.

Associated Policies:	
Biometrics Policy	Freedom of Information Policy
Data Retention Policy	Online Safety Policy
CCTV Policy *(Academy specific)*	Trust Privacy Notices
Version: 5.0	**Status: DRAFT**
Date: April 2026	**Next Review: April 2027**

Unless there are legislative or regulatory changes in the interim, this policy will be reviewed on an annual basis. The review date indicates when the policy is scheduled for evaluation and updating, not when it expires. The policy continues to apply until it is formally revised or replaced.

Version	Date	Author	Changes
V5.0	April 2026	MAHA	Policy review, in respect of SchoolPro policy V3.3 Feb 2026. Archived previous policy changes moved to end of document. Section 9 "Responding to a SAR" updated to reflect the DUAA 2025 introduction to "reasonable and proportionate" searches when locating personal data in response to a request and ICO guidance. Section 9 "Other Data Protection Rights of the Individual" updated to reflect Section 164A DPA 2018 (as amended by DUAA 2025) and associated compliant language. Section 14 'Data Protection Impact Assessments' section updated to include additional wording to clarify that DPIAs are subject to regular review. Section 15 'Data Security and Storage or Records' has been updated to include latest guidance and best practice from NCSC. Appendix 1 updated to align with best practice. References to the Chief Administrative Officer replaced with Lead Governance Professional Policy approved by the Trust Board on 7th May 2026.

Contents

1. Aims 3

2. Legislation and Guidance 3

3. Definitions 3

4. The Data Controller 4

5. Roles and Responsibilities 4

Trust Board 4

Data Protection Officer 4

Trust Executive Leadership Team 5

Principal 5

All Staff 5

6. Data Protection Principles 5

7. Collecting Personal Data 6

Lawfulness, Fairness and Transparency 6

Limitation, Minimisation and Accuracy 6

Our processing of special categories of personal data and criminal offence data 7

Conditions for processing 9

8. Sharing Personal Data 9

9. Subject Access Requests and Other Rights of Individuals 10

Subject Access Requests 10

Children and Subject Access Requests 10

Responding to Subject Access Requests 11

Other Data Protection Rights of the Individual 12

10. Parental Requests to see the Education Record 13

11. Biometric Recognition Systems 14

12. CCTV 14

13. Photographs and Videos 14

14. Data Protection by Design and Default 15

Data Protection Impact Assessments (DPIAs) 16

15. Data Security and Storage of Records 16

16. Remote Working and Data Security 17

17. Disposal of Records 17

18. Personal Data Breaches 17

19. Training 18

20. LwLAT Wellbeing Statement 18

21. Review of this policy 18

22. Archived Previous Policy Changes 18

Appendix: Personal Data Breach Procedure 20

1. Aims

1.1. The Learning without Limits Academy Trust aims to ensure that all personal data collected about staff, learners, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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

1.3. Where the 'Trust' is referred to throughout this policy, this could be referring to either the Trust itself or one, or all of its Academies, depending on the circumstances, and should be interpreted accordingly.

2. Legislation and Guidance

2.1. This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
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
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation (the Trust and its Academies) that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal 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

4.1. The Trust processes personal data relating to parents, learners, staff, trustees, governors, visitors and others, and therefore is a data controller.

4.2. The Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and Responsibilities

5.1. This policy applies to all staff employed across the Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Trust Board

5.1.2. The Trust Board has overall responsibility for ensuring that the Trust and its Academies comply with all relevant data protection obligations.

Data Protection Officer

5.1.3. The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring Trust compliance with data protection law, and developing related policies and guidelines where applicable.

5.1.4. They will provide an annual report of their activities directly to the Trust Executive Leadership Team and, where relevant, report their advice and recommendations on Trust data protection issues.

5.1.5. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

5.1.6. Our DPO is SchoolPro TLC Limited and is contactable via DPO@SchoolPro.uk

Trust Executive Leadership Team

5.1.7. The Lead Governance Professional (LGP) will act as the representative of the data controller on a day to day basis on behalf of the Executive Leadership Team.

Principal

5.1.8. Within each Academy the Principal, or their nominated representative, acts as the representative of the data controller on a day-to-day basis.

All Staff

5.1.9. Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Academy of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - 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, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - 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. Data Protection Principles

6.1. The UK GDPR is based on data protection principles that our Trust must comply with.

6.2. The principles say 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

6.3. This policy sets out how the Trust and its Academies aim to comply with these principles.

7. Collecting Personal Data

Lawfulness, Fairness and Transparency

7.1.1. We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust, as a public authority, can perform a **public task**, and carry out its official functions
- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or where the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust 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 for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- Where the above does not apply we shall request clear **consent** from the individual (or their parent/carer when appropriate in the case of a pupil)

7.1.2. For further detail of which lawful basis is used for each category of data, see the relevant privacy notice.

7.1.3. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018. This is laid out in more detail in point 7.3.

7.1.4. Where we offer online services to pupils, such as classroom apps, we rely on Public Task as a basis for processing, where this is not appropriate we will get parental consent for processing (except for online counselling and preventive services).

7.1.5. Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

Limitation, Minimisation and Accuracy

7.1.6. 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.

7.1.7. 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.

7.1.8. Staff must only process personal data where it is necessary in order to do their jobs.

7.1.9. 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 Trust's Data Retention Policy.

Our processing of special categories of personal data and criminal offence data

7.1.10. As part of our statutory functions, we process special category data and criminal offence data in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special Category Data

7.1.10.1 Special category data is defined as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Criminal Conviction Data

7.1.10.2 UK GDPR covers processing in relation to criminal convictions and offences or related security measures. This includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Appropriate Policy Document

7.1.10.3 Some of the conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance, and policies regarding the retention and erasure of such personal data.

7.1.10.4 This Data Protection Policy explains our processing and satisfies those requirements. In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notices.

Conditions for processing special category and criminal offence data

7.1.10.5 We process special categories of personal data as follows:

- Explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.
Examples of our processing include staff dietary requirements and health information we receive from our pupils who require a reasonable adjustment to access our services.

- Where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the Trust or the data subject in connection with employment, social security or social protection.

  Examples of our processing include staff sickness absences.

- Where processing is necessary to protect the vital interests of the data subject or of another natural person.

  An example of our processing would be using health information about a learner or member of staff in a medical emergency.

- For the establishment, exercise or defence of legal claims.

  Examples of our processing include processing relating to any employment tribunal or other litigation.

- Reasons of substantial public interest.

  As a Trust, we are a publicly funded body and provide a safeguarding role to young and vulnerable people. Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

  Examples of our processing include the information we seek or receive as part of investigating an allegation.

- For archiving purposes in the public interest.

  An example of our processing is the transfers we make to the County Archives as set out in our Data Retention Policy.

7.1.10.6 Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

Description of data processed

7.1.10.7 We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any union. Further information about this processing can be found in our staff privacy notice.

7.1.10.8 We process the special category data about the learners in our care and other members of our community that is necessary to fulfil our obligations as a Trust, and for safeguarding and care. This includes information about their health and wellbeing, ethnicity, photographs and other categories of data relevant to the provision of care. Further information about this processing can be found in our pupil privacy notice.

7.1.10.9 We also maintain a record of our processing activities.

Conditions for processing

Special category (SC) data

7.1.10.10 We process SC data for the following purposes:

- employment, social security and social protection.

7.1.10.11 All processing is for the first listed purpose and might also be for others dependent on the context:

- statutory purposes
- safeguarding of children and of individuals at risk

Criminal offence data

7.1.10.12 We process criminal offence data for the following purposes

- employment, social security and social protection
- statutory purposes
- regulatory requirements relating to unlawful acts and dishonesty etc
- safeguarding of children and of individuals at risk
- substantial public interest

8. Sharing Personal Data

8.1. We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a learner or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we may seek consent if necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and learners – for example, IT and communication companies, education support companies, and those that provide tools for learning. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - 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

8.2. We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- 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

8.3. 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 learners or staff.

8.4. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject Access Requests and Other Rights of Individuals

Subject Access Requests

9.1.1. Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust or one of it's Academy 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
- 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

9.1.2. It is recommended that subject access requests are submitted in writing , either by letter or email to info@lwlat.org.uk They should include:

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

9.1.3. If staff receive a subject access request, they must immediately forward it to the Principal/ nominated representative or TGP.

Children and Subject Access Requests

9.1.4. Personal data about a learner 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.

9.1.5. The ability of a child to make a request is assessed based on their competence and maturity. It is essential to determine whether the child understands their rights and the implications of the request.

9.1.6. We evaluate each request on a case-by-case basis to ensure that the child's ability to understand their rights is adequately considered. Consequently, while parents or carers may generally make SARs on behalf of their child, the child's perspective and capacity to comprehend their rights will always be considered in our decision-making process.

Responding to Subject Access Requests

9.1.7. When responding to requests, we:

- May request identification where necessary and proportionate to the request and only to the extent required to confirm an individual's identity before releasing personal data
- 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
- 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

9.1.8. We will not disclose information if it:

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

9.1.9. When responding to a Subject Access Request, we will carry out reasonable and proportionate searches to locate personal data. This means we will:

- Identify systems and records where relevant personal data is likely to be held
- Avoid excessive or irrelevant searches that would place an undue burden on the organisation.
- Take into account the nature of the request, the context of the data, and the effort required to retrieve it.

9.1.10. This approach ensures we meet our obligations while balancing practicality and fairness

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

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

9.1.13. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.1.14. The UK GDPR does not prevent a data subject making a subject access request via a third party. Requests from third parties are dealt with as follows:

- In these cases, we need to be satisfied that the third party making the request is entitled to act on behalf of the data subject.
- It is the third party's responsibility to provide evidence of this entitlement.
- This might be a written authority to make the request or it might be a more general power of attorney.
- If there is no evidence that the third party is authorised to act on behalf of the data subject, we are not required to respond to the SAR.
- However, if we are able to contact the data subject, we will respond to them directly to confirm whether they wish to make a SAR.

Other Data Protection Rights of the Individual

9.1.15. 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, where consent is the basis for processing
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- You have the right to receive information about significant decisions made solely through automated means, and to seek human review, make representations and challenge those decision
- Prevent processing that is likely to cause damage or distress
- 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)

9.1.16. Individuals should submit any request to exercise these rights to the Principal/ nominated representative or TGP. If staff receive such a request, they must immediately forward it to the Principal/nominated representative.

9.1.17. Under Section 164A of the Data Protection Act 2018, you have a statutory right to complain if you believe your personal data has been handled inappropriately.

9.1.18. If you wish to raise a concern about how we process your personal data, please contact us directly at info@lwlat.org.uk. We will acknowledge your complaint within 30 days of receipt and take appropriate steps to investigate and respond without undue delay.

9.1.19. If you are not satisfied with our response, you may escalate your complaint to the Information Commission at: Information Commissioner's Office.

9.1.20. It is important to note that the Trust could be reported to the Information Commissioner's Office (ICO) for failing to comply with their statutory responsibilities regarding SARs and other data protection rights of the individual, and penalties (including financial) may apply.

10. Parental Requests to see the Education Record

10.1. Parents, or those with parental responsibility, have a legal right to free access to their child's educational records if the child attends a maintained school.

10.2. There is no equivalent legal right to access their child's educational record if the child attends an Academy or free school in England or an independent school. Therefore, our Trust has made the decision to grant equivalent access to the parents of our learners in line with the ICO's guidance, in order to retain appropriate communication between parents and their child's Academy.

11. Biometric Recognition Systems

11.1. In the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

11.2. Where we use learners' biometric data as part of an automated biometric recognition system (for example, learners 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.

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

11.4. Parents/carers and learners have the right to choose not to use the Academy's biometric system(s). We will provide alternative means of accessing the relevant services for those learners. For example, parents/carers can pay online for school dinners and the learner gives their name at the till point.

11.5. Parents/carers and learners can object to participation in the Academy's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

11.6. As required by law, if a learner 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 learner's parent(s)/carer(s).

11.7. Where staff members or other adults use the Academy'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 Academy will delete any relevant data already captured.

12. CCTV

12.1. We use CCTV in various locations around our Academy sites to ensure they remains safe. We will adhere to the ICO's guidance for the use of CCTV.

12.2. 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.

12.3. Any enquiries about a CCTV system should be directed to the Academy Principal in the first instance.

13. Photographs and Videos

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

13.2. We will not seek consent from parents/carers for photographs and videos to be taken of their child for educational purposes for use in the classroom and Academy displays. We will process these images under the legal basis of Public Task.

13.3. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and learner.

13.4. Uses may include:

- Within the Academies, on public area notice boards and in Academy magazines, brochures, newsletters, etc.
- Outside of the Academy by external agencies such as the Academy photographer, newspapers, campaigns
- Online on our Trust or Academy websites or social media pages

13.5. 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.

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

13.7. See an individual Academy's Child Protection and Safeguarding Policy for more information on the use of photographs and videos.

14. Data Protection by Design and Default

14.1. We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- 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 law (see section 6)
- Completing data protection impact assessments (DPIAs) where the Trust's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of who has completed the training
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of the Trust and its 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.

Data Protection Impact Assessments (DPIAs)

14.1.2. A Data Protection Impact Assessment (DPIA) is a process to help us identify and minimise the data protection risks of a project.

14.1.3. We will do a DPIA for processing that is likely to result in a high risk to individuals as well as any other major project which requires the processing of personal data.

14.1.4. It is vital that the DPIA is completed before processing is commenced to ensure that all risks are identified and mitigated as much as possible.

14.1.5. Our DPIA will:

- describe the nature, scope, context, and purposes of the processing
- assess necessity, proportionality, and compliance measures
- identify and assess risks to individuals
- identify any additional measures to mitigate those risks

14.1.6. To assess the level of risk, we will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

14.1.7. We will consult our DPO and, where appropriate, individuals and relevant experts. We may also need to consult with relevant processors.

14.1.8. If we identify a high risk that we cannot mitigate, we will consult the ICO before starting the processing.

14.1.9. We will implement the measures we identified from the DPIA, and integrate them into our policies, procedures, and practice.

15. Data Security and Storage of Records

15.1. 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.

15.2. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must follow the relevant Academy procedures and ensure all records and copies are returned to the Academy
- Passwords that are at least 8 characters long containing letters and numbers are used to access Academy computers, laptops and other electronic devices. Staff and learners are reminded to change their passwords at regular intervals

- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, learners, Trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our online safety policy and /acceptable use agreements).
- 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 (see section 8)

16. Remote Working and Data Security

16.1. When accessing personal data, special category data, or financially sensitive information remotely, staff are required to ensure their network connection is secure. Open or public Wi-Fi networks must not be used for this purpose, as they present an unacceptable risk of interception or unauthorised access.

16.2. Staff working outside of the LwLAT secure network environment must connect via a private, secured network (such as a password-protected home network) prior to accessing any systems or data that fall within the scope of this policy. Failure to comply with this requirement may constitute a breach of data protection obligations under UK GDPR.

17. Disposal of Records

17.1. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

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

18. Personal Data Breaches

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

18.2. In the unlikely event of a suspected data breach, we will follow the procedure set out in the appendix.

18.3. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in an Academy context may include, but are not limited to:

- A non-anonymised dataset being published on the Academy 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 Trust laptop containing non-encrypted personal data about learners

18.4. It is important to note that the Trust could be reported to the Information Commissioner's Office (ICO) for high risk data breaches and penalties (including financial) may apply.

19. Training

19.1. All staff, trustees and governors are provided with access to data protection training as part of their induction process.

19.2. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust processes make it necessary.

20. LwLAT Wellbeing Statement

20.1. The Trust will always put the effective education of our learners at the heart of any decision that we make. In doing so, we recognise that the requirement to adhere to policies and procedures may be time consuming and can impact on workload. For this reason the Trust and its Academies will always endeavour to support staff when policies and procedures are being actioned.

21. Review of this policy

21.1. This policy is reviewed annually by the Trust. We will monitor the application and outcomes of this policy to ensure it is working effectively.

22. Archived Previous Policy Changes

Version	Date	Author	Changes
V1.0	May 2020	DENE	Original Document
V2.0	Sept 2020	JOHE/ABEV	Version updated with new roles and responsibilities
V3.0	Oct 2022	ABEV	New policy inline with model document produced by the Trust's new DPO (SchoolPro LTC) from 1st September 2022.
V4.0	Sept 2024	ABEV	Policy review, in respect of SchoolPro policy V3.0 July 2024. References to "child", "children", "student" or "pupil" updated to "learner(s)", where appropriate. Paragraph 2 – links updated to latest CCTV and SAR guidance from the ICO. Paragraph 5.4 – updated to reference Trust Executive Leadership Team and Chief Administrative Officer. Paragraph 9 - 9.1 Subject Access Requests, updated to reflect the DfE guidance on subject access requests. 9.2.2 Children and Subject Access Requests replaced and 9.2.3 added to reflect that consent should be accessed on a case-by-case basis. Paragraph 12 – reference updated to the latest ICO guidance regarding surveillance systems including CCTV. Appendix updated to reflect current roles and responsibilities for the Personal Data Breach Procedure.

			Policy approved at Trust Board meeting 26th September 2024.

Appendix: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Principal, or their nominated representative or the Trust's Lead Governance Professional (LGP)
- The Principal, their representative or the LGP, will investigate the report, and determine whether a breach has occurred. To decide, it will be considered whether personal data has been accidentally or unlawfully:

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

- The Principal will alert the LGP who will seek advice from the Trust's DPO
- The Principal will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the LGP and DPO and relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen, based on the Principal/LGP's investigation, to advise the Principal further
- The DPO, in conjunction with the LGP and the Principal, will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including, but not limited to:

  Loss of control over their data
  Discrimination
  Identity theft or fraud
  Financial loss
  Unauthorised reversal of pseudonymisation (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 will notify the ICO.

- The Principal/LGP will document the decision (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 in the Breach Log, in electronic format.

- Where the ICO must be notified, the DPO or LGP/Principal will do this via the 'report a breach' page of the ICO website. As required, the report will set out a description of the nature of the personal data breach including, where possible:

  The categories and approximate number of individuals concerned
  The categories and approximate number of personal data records concerned
  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 breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the Principal/LGP will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the they expect to have further information. The Principal/LGP or DPO will submit the remaining information as soon as possible
- The Principal/LGP will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Principal/LGP will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

  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 Principal/LGP will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Principal/LGP will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

  Facts and cause
  Effects
  Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  Records of all breaches will be stored are in the Breach-Log, in electronic format.

- The DPO and LGP/Principal will review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

An example of the actions we will take to mitigate the impact of a data breach are set out below, focusing especially on a breach involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidently made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the Principal/LGP or nominated representative as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Principal/LGP will ask the Trust IT Services to recall it
- In any cases where the recall is unsuccessful, the Principal/LGP or Academy Operations Manager will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Principal/LGP will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO/LGP will carry out an internet search to check that the information has not been made public; if it has, either the LGP or the Trust IT Team will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

Other types of breach might include:

- Details of pupil premium learners being published on an Academy website
- Non-anonymised learner data or staff pay information being shared with governors
- An Academy laptop containing non-encrypted sensitive personal data being stolen or hacked.