General Data Protection Policy and Procedure

General Data Protection Policy and Procedure

The Link Training is committed to a policy of protecting the rights and privacy of individuals, including learners, staff and others, in accordance with the General Data Protection Regulation (GDPR) established May 2018 and The Date Protection Act 2018.

The new regulatory environment demands higher transparency and accountability in how The Link Training manages and uses personal data. It also accords new and stronger rights for individuals to understand and control that use. The GDPR contains provisions that the academy will need to be aware of as data controllers, including provisions intended to enhance the protection of student's personal data.

For example, the GDPR requires that:
We must ensure that our privacy notices are written in a clear, plain way that staff and students will understand.
TLTA needs to process certain information about its staff, students, parents and guardians, employers, clients and other individuals with whom it has a relationship for various purposes such as, but not limited to:

1. The recruitment and payment of staff.
2. The administration of programmes of study and courses.
3. Student enrolment.
4. Examinations and external accreditation.
5. Recording student progress, attendance and conduct.
6. Collecting fees and payments
7. Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) TLTA must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

Compliance

This policy applies to all staff, contractors and students of TLTA. Any breach of this policy or of the Regulation itself will be considered an offence and the Academy's disciplinary procedures will be invoked.
As a matter of best practice, other agencies and individuals working with TLTA and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

The GDPR regulates the processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files, electronic records, photographs, CCTV images) and may include facts or opinions about a person.

Responsibilities under the GDPR

TLTA will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.
The academy appoints a Data Protection Officer (DPO) who is available to address any concerns regarding the data held by the academy and how it is processed, held and used.

The HR and academy support department is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the academy.

Details of the academy's notification can be found on the Office of the Information Commissioner's website. Our data registration number is: ZA024017. Certificate of registration is attached to this document.

Compliance with the legislation is the personal responsibility of all members of the academy who process personal information. Individuals who provide personal data to the Academy are responsible for ensuring that the information is accurate and up-to-date.

Data Protection Principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

1) Lawfulness, fairness and transparency
TLTA will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2) Purpose limitation
TLTA will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3) Data minimisation
TLTA will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data is given by individuals, it will be destroyed immediately.

4) Accuracy
Data processors (DPO) will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the Academy if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Academy to ensure that any notification regarding the change is noted and acted on.

5) Storage Limitation
TLTA will not retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means TLTA will undertake a regular review of the information held and implement a weeding process.
TLTA will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files).

6) Integrity and confidentiality (security)
Individuals have various rights under the legislation including a right to:

- Be told the nature of the information the Academy holds and any parties to whom this may be disclosed.
- Prevent processing likely to cause damage or distress.
- Prevent processing for purposes of direct marketing.
- Sue for compensation if they suffer damage by any contravention of the legislation.
- Take action to rectify, block, erase or destroy inaccurate data.
- Request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.
- TLTA will only process personal data in accordance with individuals' rights ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Full security measures are detailed in the procedure.

7) Accountability
TLTA and each member of staff is responsibility for complying with each of the above principles. If any member of staff comes across a breach of this, they should report this to the DPO immediately so that the appropriate action can be taken. A log of any breaches is attached to this document; these will be reviewed annually to see if any additional steps or measures should be put in place.

Consent as a basis for processing

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when TLTA is processing any sensitive data, as defined by the legislation.

TLTA understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement via the enrolment form provided by the funding provider and an additional form from TLTA, whilst being of a sound mind and without having any undue influence exerted upon them. Consent cannot be inferred from the non-response to a communication.

TLTA will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the academy. Any individual wishing to exercise this right should apply in writing to the Director. Any member of staff receiving a SAR should forward this to the Director.
Under the terms of the legislation, any such requests must be complied with within 40 days.

Additional Matters

TLTA publishes various items which will include some personal data, e.g.

- Event information.
- Photos; videos, blogs and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential or restricted access only. Therefore, it is TLTA's policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email

It is the policy of TLTA to ensure that senders and recipients of email are made aware that under GDPR, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the academy's email.

CCTV

There are some CCTV systems operating within TLTA for the purpose of protecting students, staff and property. Notices are displayed in all rooms to inform that CCTV is in operation. CCTV recordings are kept for 8 weeks for reference and can only be accessed by the management team.

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998.

Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. https://ico.org.uk/

Procedure to ensure The Link Training complies with GDPR

Students Information:

- Student information is collected from the first contact point onwards. Student will be asked to sign a consent agreement to allow us to use and process the data we are collecting, this includes information on how we will use, process, store, retain and delete their personal data.
- Personal information collected will be used to check eligibility for government funding for the training we provide. An online copy of personal data is held on our secure Cloud network, whilst the student is on programme with us. Copies of student data are also kept on our secure LMS system, OneAdvance. They take GDPR and Cyber Security. If required we can demonstrate measures taken to ensure this.
- Basic relevant personal information is taken from the students and input into our student database. This is for our administration staff to refer to for day to day running of the training academy. The database is stored securely on our cloud and required a password to access both the data base and the Microsoft share point. (Different passwords)
- Some personal information is also stored within our filing cabinets for ease of access. The filing cabinet is locked at the end of each day, the office in which the filing cabinet is stored is secured by a key code and the door into the office is fitted with a lock.
- Once consent is gained, student's personal data is shared with the DfE/ESFA This is a requirement of funding and there is a contractual agreement in place.
- Student's information can be accessed by the management and HR team, relevant information only is shared with tutors within the academy when required.
- Our safeguarding officers complete safeguarding reports when they think such action is required; the reports can contain sensitive information as well as personal information. Copies of safeguarding reports are kept securely on Microsoft Sharepoint by each DSO whilst students are on programme and these are kept securely online until the student's 25th birthday if we are the last educational provider that the student may access.
- Once a student has completed their training with us, we close down the learner on the ILR. We wait 2 months after this time to check we have received the correct amount of funding and no problems occur. After this 2 month period we destroy any hard copies of personal information and securely archive the online folder we hold on the secure server as required by theDfE/ ESFA and ESF Document Retention Guide.

(The EC or other programme authorities will audit your ESF contract. You must ensure that evidence is available to support the payments we have made to you. The main audits happen on a calendar-year basis so in the normal course of the programme you may be audited more than 18 months after we paid you. Additionally, the European Court of Auditors could audit you up to 2030.) ref: https://www.gov.uk/government/publications/esf-funding-rules

All supporting documentation evidencing the delivery of the ESF project must be kept for a period of three years from 31 December following the submission of the accounts in which the expenditure of the programme is included. The retention of Documents date is currently 31 December 2030, but you will be notified of any change to this date.

Staff Information:

- All members of staff are required to sign a declaration to consent to the information we hold, process and retain.
- We ensure that the information we hold on our staff is organised, up to date and relevant.
- Staff information is kept securely on our Microsoft cloud which only management and HR have access too.

- We hold staff information for a period of 12 months after they cease employment with The Link Training. After this time, we will destroy any information which is not relevant. We will archive basic information on past members of staff to enable us to produce references and to honour and manage any pension requirements.

Staff Training

- All staff must read and adhere to the policy. All staff are made aware of legislation changes as needed and all staff take part in annual training to refresh and update legal requirements and our workplace policies and procedures.

Record of Breaches

Date	Details of Incident	Reported By	Action Taken	Next Steps

Last Reviewed: August 2025

Signed: Amanda Lodge- Stewart Date: 18/09/2025

Director – The Link Training Academy Limited

Version control			
Last revision date:		**Next revision due: August 2025**	
Version	**Revision date**	**Author / Revewer**	**Notes**
2425V1	26/09/2024	A Lodge-Stewart	No changes
V1_2025-2026	18/09/2025	A Lodge-Stewart	**Updates to:** **SAR response time** to one calendar month Added a **Data Breach Response** section with ICO notification within 72 hours Clarified **data sharing agreements** and **DPIA** requirements Include references to **privacy notices** Addresses handling of **children's data** Mentioned **international data transfers** and safeguards.

Policy Updates for GDPR Compliance – 19/08/2025

Subject Access Request (SAR) response time

The response time for Subject Access Requests (SARs) has been updated to one calendar month in accordance with UK GDPR requirements.

Data Breach Response

In the event of a data breach, the organisation will follow a formal incident response plan. This includes assessing the breach, mitigating risks, and notifying the Information Commissioner's Office (ICO) within 72 hours if the breach is likely to result in a risk to the rights and freedoms of individuals.

Data Sharing Agreements and DPIAs

All data sharing with third parties such as DfE/ESFA, Awarding Organisations and End Point Assessment Organisations will be governed by formal data sharing agreements. Where data processing activities are likely to result in high risk to individuals, Data Protection Impact Assessments (DPIAs) will be conducted and documented.

Privacy Notices

Privacy notices for staff, students, and clients are available and clearly outline the purposes of data collection, legal bases, and rights of data subjects. These notices are accessible via the organisation's website and upon request.

Children's Data

For students who are minors, parental consent will be obtained prior to data processing. Children’s data will be handled with additional safeguards to ensure compliance with GDPR and safeguarding policies.

International Data Transfers

If personal data is transferred outside the UK or EU, appropriate safeguards such as Standard Contractual Clauses (SCCs) will be implemented to ensure compliance with international data protection regulations.