GDPR POLICY

Scope

This policy applies to all staff, including senior managers, paid staff, volunteers, sessional workers, agency staff, learners, employers and anyone working on behalf of/with **Three Dimensional Training Limited (3DT).**

Introduction

The **legal basis** for this policy is compliance with the Data Protection Act 1998 and subsequent compliance with the new Data Protection Bill which is in the process of being scrutinized in parliament before becoming an Act of Parliament. The new Act is intended to write into British law the European Union's General Data Protection Regulation (GDPR). For the purposes of this document we will refer to the Data Protection Act 1998 and any subsequent law as 'the current Data Protection Legislation'.

The Organisation needs to keep certain information about its employees, Learners and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised, and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Organisation must comply with the Data Protection Principles which are set out in the current Data Protection Legislation. In summary these principles state that the personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not to be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The Organisation and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Organisation has developed this Data Protection Policy.

Status of the Policy

This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the Organisation from time to time. Any failures to follow the policy could therefore result in disciplinary proceedings.

Any member of staff who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with the designated data controller initially (see appendix 1 for a list of current data controllers). If the matter is not resolved satisfactorily it should be raised as a formal grievance under the Organisation's agreed procedure.

Notification of Data Held and Processed

All staff, Learners and other users are entitled to:

- Know what information the Organisation holds and processes about them and why.
- Know how to gain access to any information which is covered under the current Data Protection Legislation.
- Know how to keep it up to date.
- Know what the Organisation is doing to comply with its obligations under the current Data Protection Legislation.

The Organisation will therefore provide all staff and Learners and other relevant users with a standard form of notification. For Learners this will be included on the enrolment form.

This will state all the types of data the Organisation holds and processes about them and the reason for which it is processed.

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the Organisation in connection with their employment is accurate and up to date.
- Informing the Organisation of any changes to information which they have provided, i.e. changes of address.
- Checking the information that the Organisation will send out from time to time, giving details of information kept and processed about staff.
- Informing the Organisation of any errors or changes. The Organisation cannot be held responsible for any errors unless the staff member has informed the Organisation of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about Learners course work, opinions about ability, references to other academic institutions or details of personal circumstances), they must comply with the guidelines for staff, which are set out at appendix 2.

Data Security

All staff are responsible for ensuring that:

- Any personal data, which they hold, is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal Information should be:

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerized or stored/accessed by electronic media,
- be password protected; or
- kept only on media which is kept securely.

Dealing with Potential Breaches of the Data Protection Policy

All security breaches will be reported to the Data Controller immediately.

The Data Controller will inform the individual(s) to whom the personal data relates that there has been a potential breach.

The Data Controller will then conduct an investigation to establish the extent and seriousness of the alleged breach.

The Data Controller will prepare a report on the potential breach for submission to the Principal, with recommendations for further action, if appropriate.

The Information Commissioner's Office will be informed, if appropriate.

Disciplinary action may be taken against members of staff or Learners for any such breach of data protection, under the relevant Organisation policy.

Learner Obligations

Learners must ensure that all personal data provided to the Organisation is accurate and up to date. They must ensure that changes of address, etc. are notified to personal tutors and/or the Learner Records Office and/or the Programme Management Office as appropriate.

Learners who use the Organisation computer facilities may, from time to time, process personal data. If they require further clarification, they should contact the data controller.

Rights to Access Information

Staff, Learners and other users of the Organisation have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the Organisation "Access to Information" form (Appendix 3) and give it to the data controller or their personal tutor or the Information Services office.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached.

Previously the Organisation would make a charge of £10 excluding VAT on each occasion that access is requested, although, the Organisation has discretion to waive all or part of this. However, with the introduction of GDPR this service is now free of charge except:

a) where a request from a data subject is manifestly unfounded or excessive in which case the data controller may either charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, OR
b) refuse to act on the request

The Organisation aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

All requests from the police for the release of personal data should be directed to the Data Controller, who will make the appropriate arrangements. A log of any such requests will be kept.

Publication of Whatever Organisation Information

Information that is already in the public domain is exempt from the current Data Protection Legislation. It is the Organisation policy to make relevant information available to the public, but it should be noted that the Organisation internal phone list is not considered to be a public document.

Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller.

Subject Consent

In many cases, the Organisation can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the Organisation processing some specified classes of personal data is a condition of acceptance of a Learner onto any course and a condition of employment for staff. This includes information about previous criminal convictions.

The Organisation will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The Organisation will only use the information in the protection of the health and safety of the individual but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and Learners will be asked to sign an agreement regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such an agreement can result in the offer being withdrawn.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, welfare, disciplinary, criminal convictions, race, gender and family details. This may be to ensure the Organisation is a safe place for everyone, or to operate other Organisation policies, such as the sick pay policy or equality and diversity policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and Learners will be asked to give express consent for the Organisation to do this.

Offers of employment or course places may be withdrawn if an individual refuses to consent to this without good reason. More information is available from the designated data controllers.

Examination Marks

Learners will be entitled to information about their marks for both course work and examinations at no charge. However, this may take longer to provide than other information. The Organisation may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or if all books and equipment have not been returned to the Organisation.

CCTV Tapes

CCTV Tapes are also to be considered as data for the purposes of the Data Protection policy and as such are subject to the same safeguards as any other source of personal data.

Retention of Data

The Organisation will keep some forms of information for longer than others. Because of limited storage, information about Learners cannot be kept indefinitely. Details of the length of time that particular documents will be retained is contained within the Organisations Data and Document Retention Policy.

In general, all information about staff will be kept for 10 years after a member of staff leaves the Organisation. Some information, however, about staff will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. Details of the length of time that particular documents will be retained is contained within the Organisations Data and Document Retention Policy.

Use of Artificial Intelligence (AI)

Three-Dimensional Training Limited (3DT) is committed to the responsible, ethical, and secure use of Artificial Intelligence (AI) in line with its data protection principles.

Approved AI tools, such as Microsoft Copilot and ChatGTP, may be used to support operational efficiency, reporting, and summarisation. These tools are selected for their enterprise-grade security and compliance with UK GDPR and the Data Protection Act 2018.

Only non-personal and non-confidential information may be processed using AI tools to generate summaries, insights, or reports. Personal or sensitive data will never be used in AI tools without explicit consent and appropriate safeguards.

To ensure data security and accuracy during meetings, external attendees must not use AI notetaking or transcription tools (e.g., Otter.ai, Notion AI, Fireflies.ai) unless explicitly approved by 3DT.

3DT prioritises ethical and environmentally responsible AI practices. Cloud-based, energy-efficient tools are used, and minimal, purposeful AI processing is encouraged to reduce digital waste.

All 3DT staff will complete AI awareness training. Regular audits and reviews will ensure AI use remains compliant, secure, and aligned with organisational values.

Conclusion

Compliance with the current Data Protection Legislation is the responsibility of all members of the Organisation. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to the Organisation facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be directed to a designated data controller.

APPENDIX 1

The Data Controller and the Designated Data Controller/s

The Organisation, as a body corporate, is the data controller under the Data Protection Act, and is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day to day matters.

The Organisation has a designated lead data Controller.

Rachael Davies, Director of Three Dimensional Training Limited

APPENDIX 2

STAFF GUIDELINES FOR DATA PROTECTION

All staff will process data about Learners on a regular basis, when marking registers, or other similar work, writing reports or references, or as part of a pastoral or academic supervisory role. The Organisation will ensure through registration procedures, that all Learners give their consent to this sort of processing, and are notified of the categories of processing, as required by the current Data Protection Legislation. The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

- General personal details such as name and address.
- Details about class attendance, course work marks and grades and associated comments.
- Notes of personal supervision, including matters about behaviour and discipline

Information about a Learner's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the Learners consent. If a member of staff needs to record this information, they should use the Organisation standard form.

E.g.: recording information about dietary needs, for religious or health reasons, prior to taking Learners on a field trip; recording information that a Learner is pregnant, as part of pastoral duties.

All staff have a duty to make sure that they comply with the data protection principles, which are set out in the Organisation's Data Protection Policy. In particular, staff must ensure that records are:

- Accurate.
- Up-to date.
- Fair.
- Kept and disposed of safely, and in accordance with the Organisation policy.

The Organisation will designate staff in each area as 'authorised staff'. Except where specifically designated these 'authorised staff' will be the Organisation Managers or Senior Management. These staff are the only staff authorised to hold or process data that is:

- Not standard; or
- Sensitive.

The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:

- In the best interests of the Learner or staff member, or a third person, or the Organisation; and
- He or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all circumstances.

This should only happen in very limited circumstances eg a Learner is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the Learner is pregnant or a Jehovah's Witness.

Authorised staff will be responsible for ensuring that all data is kept securely.

Staff must not disclose personal data to any Learner, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with Whatever Organisation policy.

Staff shall not disclose personal data to any other staff member except with the authorisation of the designated data controller, or in line with the Organisation's Data Protection Policy.

Before processing any personal data, all staff should consider the checklist.

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the data subject's express consent?
- Has the Learner been told that this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the Learner or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

APPENDIX 3

The Organisation Access to Information Form which satisfies the Organisation's Data Protection Policy is to be found overleaf.

ACCESS TO INFORMATION

This form satisfies the requirements of the Organisation's Data Protection Policy

YOUR DATA	
All persons requiring Access to Personal Data in line with the Organisation Data Protection Policy should provide proof of identity.	
Reference Number (if known)	
Surname	
Forenames	
Date of Birth	

TO BE COMPLETED BY ORGANISATION STAFF		
Proof of Identity Checked	Please Tick as appropriate	
	YES	NO
Member of Staff Signature		
Member of Staff Name (Please Print)		
Date		

SUPPLEMENTARY INFORMATION
Please describe briefly below what data you wish to access and sign the declaration below

DECLARATION: The information I have supplied on this form is correct as far as I am aware.	
Signature (person applying for data access)	
Date	

POLICY END

Policy Updated: **Sep 2025**

Version Number: **V10**

Updated by: **Vicky Fearnley**

Date for review: **Sep 2026**