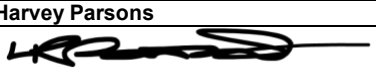
Data Protection Policy

This Revision Number and Effectiveness Date	**Issue 7 Dated 12-09-2025**
Department	**Quality Assurance Department**
Policy Author	**Harvey Parsons**
Date of Last Review	**September 2025**
Next Review Date	**September 2026**
This Version is Reviewed and Issued by	**Harvey Parsons**
Signature	
Position within GLP	**Data and Quality Compliance Director**

1. Introduction

GLP Training takes its responsibilities under the Data Protection Act 2018 ('the Act') and similar regulations across Mainland Europe very seriously. These regulations impose restrictions on how we may use personal information.

This data protection policy sets out the roles and responsibilities of employees and companies within the GLP Training with regard to the processing of personal information.

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process (i.e. use) personal information about our staff, customers, suppliers and others that we communicate with and we recognise the need to treat it in confidential, secure and lawful manner.

Personal information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards. In the UK, these are specified in the Act and other regulations, which implement the EU Directive on Data Protection.

We may process all the information we obtain from you to enable us to fulfil our contractual obligations to you and we may request further information from third parties or disclose your details to other selected third parties, such as the Department for Education, Awarding Organisations, the Learner Record System and Ofsted.

Access to all data systems, paper based or electronic is strictly controlled with access to either system granted only after the relevant security checks have been completed and only after a GLP Systems Access Form has been completed and approved. Access requests MUST be made by the person requiring access, for GLP, this must be the requesters line manager, for external requests, the request must be made by the persons who requires access only, third party requests will not be granted.

Guest Access, employers, Ofsted, DfE, ESF and Awarding bodies representatives will only be given access to data systems on the completion of a GLP Systems Guest Access form, this form must be completed and approved before access is granted and will be limited to the required time duration request by the guest or deemed necessary by the GLP Data and Compliance team only. The level of access granted will be set dependant on the guest requesting access, i.e., DfE-full access, Awarding Body EQA-limited access to evidence portfolios only.

As soon as the time allotted has lapsed the access granted will be revoked and must be recorded as such.

In disclosing your personal details to us, you agree that we may process and in particular may disclose your personal data.

- as required by law to any third parties
- to selected third parties who may process personal data on our behalf
- to third parties such as the Department for Education (DfE), Awarding Organisations, Learner Record System (LRS) or Ofsted, who may use your personal data or sensitive personal data (as appropriate) to enable us to fulfil our contractual obligations to you.
- carry out statistical analysis
- pass to their regulator or industry bodies for the following purpose

(1) monitor equal opportunities relating to ethnicity or disability, or for other such monitoring purposes.

(2) account for candidates where there is a requirement to do so.

(3) where there is a requirement for such bodies to contact a candidate directly and the information is not readily accessible by other means.

This policy will provide you with sufficient information, instruction and training for you to know how to identify personal information and process it appropriately. You should also read GLP Training policy relating to the use of social media and should understand GLP Training's guidelines on information security.

You should make sure that you are fully aware of this policy and that you comply with its directions. If we fail to comply with the Act, we may face legal penalties and fines and, in some circumstances, individuals may be held personally liable.

You should be aware that any breach of this policy will be taken seriously and may result in disciplinary action being taken which may result in the incident being forwarded to the relevant external authorities.

This policy is in accordance with the DBS policy on data protection, as set out in the GLP Training Ltd Management Handbook.

2. Data protection: core principles

The Act outlines eight core principles which broadly set out the way in which personal information should be used. These provide that personal information must be:

- processed fairly and lawfully.
- processed for limited purposes and in an appropriate way; be obtained only for one or more specified and lawful purposes and should not be processed in any manner incompatible with that purpose or those purposes.
- ALL GLP systems users must be approved before access is given at the appropriate level for the user's scope of operation, access is granted only when a completed GLP Employee Systems Access Form has been completed, submitted, and approved, approval can only be given by the GLP Training Data Protection Officer (DPO) or Managing Director. Guest access for employers or external auditors is granted via the GLP Systems Guest Access form and follows the same approval route as above, guest access is removed once the stated access time has expired.

- Increased or reduced access to the GLP Data Systems must be requested in writing via the relevant Systems Access form and be approved before any such changes in user rights is implemented.
- adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
- accurate and, where necessary, kept up to date.
- not be kept for longer than is necessary for that purpose or those purposes.
- processed in accordance with the rights of Data Subjects under the Act.
- secure, meaning that appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information; and
- not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.
- If you comply with GLP Training's policy, you will also comply with the principles above and therefore keep within the law.
- The Department for Education and Awarding Organisations may also transfer your personal information outside the European Economic Area, but GLP Training will use all reasonable efforts to ensure that any such transferred information is given the same protection and levels of security as if it were being processed within the UK.
- GLP Training operate a "Clear Desk" policy which is strictly enforced by routine and ad hoc patrols of all building departments, operational building areas and desks. Failure to ensure that the "Clean Desk" policy is enforced can result in disciplinary action being taken.

Key definitions "Personal information"

is data about a living individual who can be identified: -

• from the data; or

• from that data and other information which is in the possession of or is likely to come into the possession of the Data Controller.

Personal information includes any expression of opinion about an individual and any indication of the intentions of the Data Controller or any other person in respect of the individual. Note the definition does not cover companies (although it does cover individuals within companies), nor does it cover information about the deceased.

Sensitive personal information"

Includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal information can only be processed under strict conditions and will usually require the express consent of the person concerned.

Storage of data

All GLP Training computers systems are password protected. Workstation passwords are strictly controlled and only known to the Data Protection Officer and Administration Manager and system operator, and relevant workstation operative only. Passwords for all computer systems, internal and external software applications and funding partner system access are securely stored by the Data Protection Officer. The issue of these passwords is strictly controlled and only passed to users with

the necessary need to access said systems. Accounts system passwords are only available to the Managing Director and Head of Finance.

Internet and computing systems security and monitoring is contracted out to SMH IT Solutions Worcester, Monthly reports on systems performance, usage and security threats are generated and reviewed and any identified actions that are or could be a threat to the integrity or security of the systems are actioned immediately.

The hosted data and e-Portfolio system (BUD Systems Ltd) are managed via the GLP Employee Access and GLP Guest Access approval system. Master Administration rights for these systems are only approved by the Data protection Officer or CEO. Multifactor Authentication is operated on this system for all users who have access to the main data storage area.

Any redundant or unrequired paper documentation printed or received that contain personal data, whether company, employee, funding partner or learner are placed in the confidential document storage bin to await collection and secure destruction by the secure document destruction contractor, GLP Training Ltd have a contract with "Shreddit Ltd" for secure document destruction. Secure document bins are present in all operational offices, they key to these boxes are controlled by the Head of Administration.

Other policies that operate in conjunction with this Policy are:

GLP-POL-0041	Document Retention and Archiving Policy
GLP-POL-0044	Privacy Policy
GLP-POL-0055	Information Security Policy
GLP-POL-0031	Information Systems Incident Management Policy
GLP-POL-0015	Information Systems Access Policy

This policy will be reviewed regularly to ensure that any changes in the Data Protection Act 2018 are incorporated and to ensure GLP Training Ltd comply with said Act.