Professional Training Solutions
Data Protection (GDPR), Security and Confidentiality Policy

In order to comply with the Data Protection Act 1998 and subsequently The General Data Protection Regulations 2018. Professional Training Solutions Ltd will ensure that all personal data relating to all internal and external stakeholders is held securely.

Professional Training Solutions are registered with the Information Commissioners' Office (ICO) – Certificate No: Z1072279.

Professional Training Solutions Data Protection Officer is Samantha Cary, Data and Compliance Manager; and can be contacted by email: s.cary@protrain-solutions.co.uk; or by telephone on 01252 712945.

Introduction:
We regard the lawful and correct treatment of personal information held by Professional Training Solutions as critical to successful operations and for maintaining confidence between ourselves and those whom we deal with. We are committed to protecting the rights and freedoms of data subjects, and safely and securely processing their data in accordance with all of our legal obligations.

Professional Training Solutions within its organisation needs to gather and use certain personal information about individuals. In addition to having the personal information relating to our employees, this can include employers, learners, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled, and stored to meet the company's data protection standards — and to comply with the law. We fully endorse and adhere to the principles of data protection, as detailed in the Data Protection Act 2018 and from 25 May 2018, the General Data Protection Regulation.

Why This Policy Exists:
This data protection policy ensures Professional Training Solutions complies with data protection law and follows good practice. We endeavour to protect the rights of staff, our learners, customers and partners at all times, and are open and transparent with all parties about how we store and process individuals' data and protects ourselves from the risks of a data breach.

This policy sets out how we ensure ongoing confidentiality, integrity, availability and resilience of our processing systems and services, and how we comply with the rights of data subjects in respect of receiving privacy information, and access, rectification, deletion and portability of personal data.

Data Protection Law:
The Data Protection Act 1998 and subsequently the General Data Protection Regulation May 2018; describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

We ensure all personal data complies with the eight principles outlined in The Data Protection Act:

- Be processed fairly and lawfully.
- Be obtained only for specific, lawful purposes.
- Be adequate, relevant, and not excessive.
- Be accurate and kept up to date.
- Not be held for any longer than necessary.
- Processed in accordance with the rights of data subjects.
- Be protected in appropriate ways.
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Policy Scope:
This policy applies to:

- The head office and all offices of Professional Training Solutions.
- All staff including freelance tutors and assessors, suppliers, volunteers, subcontractors and partners working on behalf of Professional Training Solutions.
- All learners and clients involved with Professional Training Solutions.

This policy supplements our other policies relating to internet and email use for both staff and learners, and CCTV for which we have a separate policy which should be read in conjunction with this policy.

It applies to all data that the company holds relating to identifiable individuals including names, addresses, email addresses, telephone numbers plus any other information relating to individuals.

Data Protection Risks:
This policy is to protect Professional Training Solutions, along with all internal and external stakeholders, from all data security risks, including but not limited to:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Breaches:
Any personal data breaches will be reported immediately to the Data Protection Officer. If the DPO deems that the breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), they will inform the Information Commissioner's Office without delay, and in any event, within 72 hours. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.

Responsibilities:

Everyone who works for or with Professional Training Solutions has some responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The Board of Directors is ultimately responsible for ensuring that Professional Training Solutions meets its legal obligations.

The Data and Compliance Manager is the nominated Data Protection Officer and is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule as set out in the Document Retention Policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Professional Training Solutions holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring data is deleted according to our Document and Data Retention Policy.
- Maintain Professional Training Solutions ICO Registration.
- Use of CCTV is line with the CCTV policy.
- Implementing all GDPR and confidentiality processes and procedures.
- Ensuring our privacy policy is outlined on our website and all relevant documents.
- Ensuring the updated policy and procedure is available on our website and on all policies and procedures available to our internal and external stakeholders.

The HR Executive is responsible for:

- Arranging data protection training and advice for the people covered by this policy, including protocols in emails, sending data.
- Ensuring all new staff starters within the business are aware of their GDPR requirements.
- Destroy personal data according to our Document and Data Retention Policy.

The IT Director is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards, including PICS, OneFile and our outsourced IT Support Company.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Investigating of any breaches of IT Security.
- Providing secure methods of transferring authorised personal data.
- Back up data and disaster recovery procedures.
- Virus detection and hacking preventative measures.
- Ensuring all software and data is wiped from old IT equipment before disposal.
- Testing, assess and evaluating of the processes and systems put in place to evaluate the effectiveness of all GDPR, confidentiality systems and services.

The Data & Compliance Manager is responsible for:

- Ensuring all subcontractors have a robust GDPR and Data Protection Policy.
- Ensuring all subcontractors are registered with the ICO.
- Ensuring all data sent is password protected.

The Directors, are responsible for:

- Approving any data protection statements attached to communications such as emails and letters, learner applications.
- Addressing any data protection queries
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Ensuring this policy is updated and reflects current legislation and working practices.
- Ensuring processes and procedures are in place to test, assess and evaluate the effectiveness of measures implemented to sure GDPR compliance.

General Staff Guidelines:

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

Professional Training Solutions will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- Strong passwords must be used, and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager or the Data Protection Officer if they are unsure about any aspect of data protection.

All Professional Training Solutions staff are responsible for:

- Checking that any information that they provide in connection with their employment is accurate and up to date.
- Informing of any changes to information, which they have provided. I.e., changes of address.
- Checking the information sent out from time to time, giving details of information kept and processed about staff.
- Only have access to personal data in which they have a legitimate business interest.
- Informing of any errors or changes. Professional Training Solutions cannot be held responsible for any errors unless the staff member has informed them.
- Ensuring all personal data which is held off site relating to any internal or external stakeholders is kept securely (locked filing cabinet/drawer/on the network).
- Not disclosing any personal data which they hold on to students (orally, in writing or electronically) to an unauthorised third party without the prior consent of the Data Protection Officer or a Director.

- Ensuring that any data approved for disclosure and sent electronically must be password protected and passwords sent separately.
- Inform the Data Protection Officer of any proposed new uses of personal data.
- Ensuring that if and when, as part of their responsibilities, staff collect information about other people, (i.e., about students' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines contained in this policy.
- Destroying personal data according to our Data Retention Policy.
- Computer screens are always locked if left unattended for a long period.
- All accounts are password protected using strong encryption.
- Learners' personal data is not shared with other parties except as necessary in delivering care or preventing crime.
- Copying data and/or software and file sharing is forbidden without prior authorisation from Senior Management.

All Professional Training Solutions Managers are responsible for:

- Ensuring they are satisfied with the legality of holding and using the information collected by staff in their area.
- Ensuring that the use of personal data complies with all appropriate policies.
- Ensuring that relevant staff they manage, undertake the GDPR training.
- Referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations without delay.

Learners are responsible for:

- Checking that the information they provide in connection with their enrolment is accurate and up to date.
- Informing of any changes to the information they provide, such as, change of address, emergency contact details are notified using the "Correction of Personal Information" form.
- Ensuring that any personal data which they are required to provide as part of their enrolment is not disclosed (orally, in writing or electronically) to an unauthorised third party.
- Not seeking to gain unauthorised access to personal information. Complying with all policies regarding the use of IT facilities.

Data Storage:

When data is stored on paper, it will be kept in a secure place where unauthorised people cannot see it, this includes locked filing cabinets in head office.

All staff should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion, and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- Data should never be stored on removable media (eg CD/DVD/USB).

- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use:
When working with personal data, employees should ensure the screens of their computers are always locked when left unattended. All laptops and machines should be password protected, and this should not be removed.

Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure. Any personal data shared should be sent by password protected documents, and where appropriate large files sent via WeTransfer.

Data must be encrypted before being transferred electronically.

Personal data should never be transferred outside of England.

Data Accuracy:
Professional Training Solutions is required by law to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated. For instance, by confirming learner's details when they call.

Data should be updated as inaccuracies are discovered. For instance, if a learner can no longer be reached on their stored telephone number, it should be removed from the database.

It is the responsibility of the Associate Director for Sales and Marketing to ensure marketing databases and Salesforce are checked against industry suppression files every six months.

Subject Access Requests:
All individuals who are the subject of personal data held by Professional Training Solutions are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

Subject access requests from individuals should be made by email, addressed to the Data & Compliance Manager: s.cary@protrain-solutions.co.uk.

The Data Protection Officer can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £25 per subject access request. The Data Protection Officer will aim to provide the relevant data within 14 days.

The Data Protection Officer will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data For Other Reasons:
In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Professional Training Solutions will disclose requested data.

However, the Data Protection Officer will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Consent:
We process data on the basis of informed consent. All data subjects (e.g., staff, service users, volunteers) are informed that records of their dealings with the company (e.g., training records, employment records) are kept and processed electronically, and are asked to sign to give their consent, either in a separate consent form or a dedicated consent section of other forms. Signed consents are kept on file, and are readily auditable.

Data Transfers:
All data is kept securely on the cloud, using servers located in the United Kingdom. If it should become necessary to transfer personal data outside the UK. Our GDPR Policy and Procedures document provides for this in terms that comply with GDPR regulations.

Record Keeping:
We maintain a central record of all personal data collected, held, and processed as part of delivering our services to ensure full compliance with the requirements of GDPR. We keep records of personal data processing that may be considered "high risk", for example:

- Personal data processing that could result in a risk to the rights and freedoms of data subjects; or
- Processing sensitive personal data or data concerning criminal offences and convictions.
- Information required for privacy notices (aka "privacy information", "privacy policy" etc).
- Records of consent.
- Contracts with data processors.
- The location of personal data.
- Reports of Data Protection Impact Assessments.
- Records of personal data breaches; and
- Information required for the processing of special category personal data or criminal offence data under the Data Protection Act 2018.

Providing Information:

Professional Training Solutions aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

Professional Training Solutions has a Privacy statement, setting out how data relating to individuals is used by the company.

Rights of Individuals:
Individuals have rights to their data which we will respect and comply with to the best of our ability. We will ensure individuals can exercise their rights in the following ways:

Right to Rectification:
We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete. This must be done without delay and no later than one month.

Right to Erasure:
We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

Right to Restrict Processing:
We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.
- Right to data portability
- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.
- Right to object
- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.
- Rights in relation to automated decision making and profiling
- We must respect the rights of individuals in relation to automated decision making and profiling.
- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Right to be Informed:
Providing privacy notices which are concise, transparent, intelligible, and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children. Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency. All data subjects are informed of their rights at the point of collection and reminded via saff/learner/user handbooks, and any relevant correspondence.

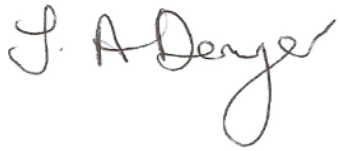
Right of Access:
Enabling individuals to access their personal data and supplementary information and allowing individuals to be aware of and verify the lawfulness of the processing activities.

Data Retention:
We will retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but will be determined in a manner consistent with our Document and Data Retention policy guidelines.

Testing:
GDPR compliance is assessed once a year, and covers:

- What data we are collecting.
- Location for storing the data.
- How data is protected.
- How long data is kept for.
- How we honour requests to delete data.

This Policy has been agreed by
Jackie Denyer, Managing Director



Date Signed: 22nd February 2023