Data Protection Policy

1. POLICY STATEMENT

The Procurement Academy (TPA) needs to collect and use certain types of information about the applicants, learners, employers, employees, suppliers, and other stakeholders for a variety of business purposes.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards and comply with the Data Protection Act 1998 and General Data Protection Regulation (GDPR) from May 2018.

2. SCOPE

This policy applies to all staff.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Our Data Protection Officer (DPO), Philip Chippindale has overall responsibility for the day-to-day implementation of this policy.

The Procurement Academy is the Data Controller under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. PROCEDURES

Fair and lawful processing
TPA will process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by The Apprentice Academy
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly

Data Protection Policy

Responsibilities of all Managers in The Procurement Academy

- Approving data protection statements attached to emails.
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers and employees
- Highlights that our work may require us to give information to third parties such as professional advisers
- Provides that customers have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work or safeguarding). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data Protection Policy

Staff personal data

All staff must take reasonable steps to ensure that the personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security

All staff must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- Data should only be stored on designated drives and servers, and should only be uploaded on approved cloud computing services
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data use

- When working with personal data, employees should ensure the screens of computers are locked when left unattended
- Personal data should not be shared informally. In particular, it should never be sent by e-mail, as this form of communication is not secure
- Data must be encrypted before being transferred electronically
- Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data

Data Protection Policy

Data retention

TPA staff must 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 should be determined in a manner consistent with our data retention guidelines.

Our contracts with the Education and Skills Funding Agency stipulate specific timeframes that data must be held for auditing purposes.

Data Accuracy

The law requires TPA to take reasonable steps to ensure data is kept accurate and up to date, which we will do.

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

Subject access requests

Under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. Such as

- 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 and addressed to the DPO. The DPO can supply a standard request form, although individuals do not have to do this.

Individuals will be charged £10 per subject access request. The DPO will aim to provide the relevant data in 14 days

The DPO will always verify the identity of anyone making a subject access request before handing over any information

Processing data in accordance with the individual's rights

All staff should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Staff must not send direct marketing material to someone electronically (e.g. via email) unless they have a business relationship with them.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

Data Protection Policy

Staff Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process.

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
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
- In particular, 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 DPO if they are unsure about any aspect of data protection

DOCUMENT CONTROL				
VERSION	DATE OF ISSUE	DATE OF REVIEW	DATE OF NEXT REVIEW	SIGNATURE
4	August 2018	July 2025	July 2026	*Philip Chippindale*