THE APPRENTICE and TRAINING PARTNERSHIP

DATA PROTECTION POLICY

The Apprentice & Training Partnership ("The ATP") needs to gather and use certain information about individuals. These can include learners, customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. The ATP uses this data to monitor performance, achievements, Health and Safety, Equality, Diversity and Inclusion, Safeguarding, 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 the UK Government complied with.

1 Scope of the Policy

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the Data Protection Act [1998] ("The Act").

This data protection policy ensures The ATP:

- Complies with data protection law and follow good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes individuals' data.
- Protects itself from the risks of a data breach.

2 Data Protection Law

The Act describes how organisations – including the ATP – 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. The Act is underpinned by eight important principles.

These say that personal data must:

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

The Apprentice and Training Partnership is a trading name of Technical Professionals Limited Company No. 06161067, Registered Office c/o RPG, 62 Wilson Street, London, EC2A 2BU. Please note that this policy was last updated on 07th December 2016.

3 What rights do individuals have?

Under the Act, individuals have specific rights:

- Right of access – individuals have a right to know what information organisations hold about them on a computer or in certain filing systems and should be aware how to gain access to it and how to keep it up to date. Individuals can submit a Subject Access Request to see or have a copy of this information. The ATP has 40 calendar days to respond.
- Right to prevent direct marketing – individuals have the right to object to their personal information being used to target them with unwanted marketing.

4 Processing Data

The ATP is registered with the Information Commissioner's Office (ICO) **ZA193080**, to process (this means obtain, hold, record or carry out any operation on the data) specific personal data. To comply with the Act, The ATP will only collect and use personal data that is covered by its register entry.

The ATP will take appropriate measures against unauthorised and unlawful processing of personal data and accidental loss or damage to personal data by ensuring that the personal data is held in a secure manner thereby protecting confidentiality.

In many cases, the ATP can only process personal data with the consent of the individual. Agreement to the ATP processing personal data contained within the ATP's "*Eligibility and Application form"*, or other data provided by the learner during the course of their programme with the ATP, is subject to a declaration on the ATP's "*Eligibility and Application Form"* which is signed by the learner.

Agreement to the ATP processing personal data is also a condition of employment for staff. This includes information about current or previous spent criminal convictions.

The ATP may also ask for information about particular health needs of staff and students, such as allergies to particular forms of medications, or learning difficulties and/or disabilities conditions. The ATP will only use the information in the protection of the health and safety of the individual.

5 Transferring Data

As mentioned above, The ATP collects a wide range of personal data relating to staff and students for its own purposes, and to meet external obligations. This may result in the eventual transfer of personal data to an outside third party, however any such transfers must be permitted under the Act.

- Personal data must not be disclosed to unauthorised third parties. Unauthorised third parties includes another individual or organisation, family members, friends, local authorities, government bodies, and the Police where the individual has not consented to the transfer unless disclosure is exempted by the Act, or by other legislation. There is no general legal requirement to disclose information to the Police.

However, data can sometimes be disclosed without consent, where, for example, it is required for:

- Protecting the vital interest of the data subject (i.e. release of medical data in an emergency).
- The prevention or detection of a crime.
- Normal reasonable business.

Personal data can be transferred to another third party if the data subject has given their consent. This must always be in writing. Consent cannot be inferred from silence, so if the ATP requests consent so that personal data can be provided to a third party, and no response is received, the ATP must infer that consent is withheld.

Often a third party, or prospective employer, may contact the ATP to verify details about a learner, such as examination results etc.… In most circumstances learners would not object to the disclosure of such information, and indeed it may be beneficial to the learner. However, the request for information should be accompanied by a statement from the learner consenting to the disclosure, or the student should be contacted to confirm their consent.

The ATP will disclose information in accordance with any legislation which it is subject to.

Transferring data securely

Reasonable effort should be made to ensure that any data being transferred, regardless of whether electronic or otherwise, remains secure. Once authorisation has been given to transfer data externally, then the most appropriate, secure method of transfer will be used. The originating member of staff should confirm safe receipt of the information from the recipient and highlight any potential losses to the Data Protection Officer immediately.

6 Subject Access Requests and monitoring and review

All individuals who are the subject of personal data held by the ATP 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.

If an individual contacts the ATP requesting this information, this is called a Subject Access Request.

Subject access requests from individuals should be made by email, addressed to the data controller at info@theatp.org.uk. The data controller can supply a standard request form, although individuals do not have to use this.

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

A record is kept of all the data protection requests made of the ATP and the timescales for response are monitored to ensure that the ATP meets its commitment to respond to requests within the 40 calendar days specified by the ICO.

The ATP data procedures are reviewed by the ATOs internal and external auditors to ensure that information is held securely.

7 Responsibilities

Everyone who works for or with the ATP 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 is ultimately responsible for ensuring that the ATP meets its legal obligations.

All staff are responsible for:

- Checking that any information that they provide to the ATP in connection with their employment is accurate and up-to-date.
- Informing the ATP of any changes to information, which they have provided i.e. change of address.
- Informing the ATP of errors or changes. The ATP cannot be held responsible for any errors unless the staff member has informed The ATP of them.
- Ensuring that personal data which they hold on learners is kept securely (locked filing cabinet, drawer, on the network).
- Not disclosing any personal data which they hold on learners (orally, in writing or electronically) to an unauthorised party without the prior consent of the Data Protection Officer.
- 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 learner's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the above guidelines.
- Destroying personal data according to the Data disposal information in section 9.

Learners are responsible for:

- Checking that information they provide to the ATP in connection with their enrolment is accurate and up-to-date.
- Informing the ATP of any changes to the information they provide, for example, change of address, emergency contact details are notified using the appropriate form which is available from Administrative Services. This will enable the ATP to update their Management Information System.
- Ensuring that any personal data which they be required to collect as part of the application to the ATP is not disclosed (orally, in writing or electronically) to an unauthorised 3rd party.
- Not seeking to gain unauthorised access to personal information.
- Complying with all ATP policies regarding the use of IT facilities.

Managers are responsible for:

- Ensuring they are satisfied with the legality of holding and using the information collected by staff in their areas.
- Ensuring that the use of personal data complies with all appropriate ATP policies.
- Ensuring that relevant staff they manage attend the Data Protection training.
- Referring any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer.

IT services are responsible for:

Whilst all staff and users of personal data have some responsibility for the security of data, IT and MIS staff have an important role in ensuring the security of computerised data. They will:

- Be responsible for advising the ATP on the state of technological development with regard to IT security.
- Provide secure methods of transferring authorised personal data outside the ATP.
- Back up data on the ATP IT systems and have disaster recovery procedures in place.
- Implement virus detection and hacking preventative measures.
- Through liaison with the appropriate manager, ensure that the ATP business systems are secure and appropriate restrictions on access to personal data in which they have a legitimate business interest.
- Require the use of passwords and ensure that they are changed regularly.
- Produce and update policies for the use of the ATP including email, intranet and internet.
- Investigate breaches of IT security.
- Ensure that data is deleted according to the ATPs data disposal information in section 9.

Human Resources will:

- Ensure that Data Protection obligations are reflected in the ATP Disciplinary Procedures and Contracts of Employment.
- Ensure that all staff are aware of the types of personal information that the ATP will process on them and ask staff to check this information as required.
- Ensure that all obligations outlined within the DBS Code of Practice are adhered to.
- Provide advice to managers and others on the application of DBS Code of Practice.
- Destroy personal data according to section 9.

8 The Data Protection Officer

The ATP as a corporate body is the data controller under the Act. However, the designated data protection officer will deal with day to day matters. The ATP designed data protection officer is:

Katie Luckett
Operations Associate

Overall responsibility for the policy is:

Martin Burr
Director

The ATP data protection officer will:

- Maintain the ATP Data Protection Notification.
- Liaise with the ICO and the ATP legal advisors as required.
- Make recommendations to the Board regarding Data Protection Policy and good practice.
- Provide general guidance and advice and dissemination of information regarding data protection.
- Arrange data protection training and advice for the people covered by this policy.
- Check and approve contracts or agreements with third parties that may handle the Company's sensitive information.
- Ensure all systems, services, equipment used for storing data meet acceptable security properly.
- Evaluate any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approve any data protection statements attached to communications such as emails and letters.
- Deal with subject access requests and co-ordinate responses.
- Co-ordinate and advise on all non-routine requests for disclosure of personal information.
- Monitor and report on data protection requests.

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

9 Disposal of information

The ATP and all its staff and members have an obligation to dispose of personal, confidential and business critical information in a secure manner.

For confidential paper information, staff should ideally cross shred onsite and additionally put in to the confidential waste disposal.

For confidential, electronic information:

- DVDs/CDs should be shredded and then put in the recycling stream.
- Computer hard drives and external storage media (such as USB sticks) should be wiped with a suitable software tool. No unencrypted data should be left on these types of media before re-using/ recycling/ disposing.
- Media that cannot be wiped initially will need to be sufficiently protected before being overwritten e.g. in a locked safe.

This document should be read in conjunction with:

Safeguarding Policy
Equality, Diversity and Inclusion Policy
Health and Safety Policy