DATA PROTECTION POLICY

*V2 Dec 2021

Introduction

The Data Protection Act, 1998 (the "DPA") governs the way in which we, as a business, are required to handle, manage and store data on individuals. Failure to comply with the DPA can result in serious consequences, including monetary fines, for both the Company and certain individuals. Marshall Assessment is fully committed to compliance with the DPA. Under UK' data protection laws (GDPR) you have a number of rights in respect to the processing of any personal information. The aim of this policy is to describe how the Company will fulfil its obligations, in compliance with applicable data protection law, in particular the General Data Protection Regulation (EU) 2016/679 (GDPR).

The Data Protection Principles

The DPA sets out 8 Principles of data protection. Marshall Assessment fully endorse the 8 Principles and considers the lawful and correct treatment of personal information as important to the success of the business. We aim to ensure adherence to the DPA and the 8 Principles by the adoption of strict processes and controls which will be in place throughout the business.
The 8 Principles require that personal information shall:
1. Be processed fairly and lawfully;
2. Be obtained for one or more specified and lawful purposes and shall not be processed in any manner incompatible with that purpose or those purposes;
3. Be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for the specified purpose(s);
6. Be processed in accordance with the rights of data subjects under the Act;
7. Be subject to appropriate technical and organisational measures to prevent the unauthorised or unlawful processing of personal data or the accidental loss, damage or destruction of, or damage to, personal data; and
8. Not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures that an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Scope

This policy applies to all personal information of individuals obtained, held, stored, processed, used or shared by Marshall Assessment. All employees will be required to comply with the 8 Principles and the DPA including any applicable procedures or processes adopted by the Company in relation to personal data.

Roles and Responsibilities:

Director

The Directors shall have overall responsibility for data protection compliance across the business. Responsibilities include:

- ensuring suitable resources and direction are given to data protection issues;
- monitor, via reporting from staff and the nominated Data Protection lead person, the effectiveness of data protection systems within the business.

Employees/Assessors

All employees must

- Familiarise themselves with the data protection policies and procedures affecting their work.
- Fully support the business in the implementation of data protection policies and procedures of the business; and report any data protection incidents to their line manager.

Nominated Data Protection Lead Person - (Robert Green)

This is the person nominated by the business from time to time and who is deemed competent in the area of data protection. The nominated Data Protection lead person shall be responsible for:

- Communicating any changes in data protection legislation and requirements which the business must fulfil;
- Provide advice and support to the business on data protection requirements;
- Maintain a log of all data protection incidents and reporting of such incidents to the Information Commissioner's Office.

End Point Assessment Declaration forms-
What information is collected?

During the enrolment process we gather the learner's name, home address, work address, date of birth, unique learner number, contact information (phone and email). This information is all located on our Office 365 Sharepoint site and a copy on their ACE360 pages of our MIS both of which are securely stored in the cloud, of which only the administration team have access to.

We need to share learner's personal data with organisations that are involved with either the quality or governance of apprenticeships, awarding organisations and the Education and Skills Funding Agency. These organisations need the data to ensure that the learners are eligible for the programmes they are studying, to ensure they receive their certificates and so that the quality of provision they receive is of a high standard. This is a requirement set by the government in order to register learners onto their qualifications. In some circumstances we may have to disclose learner's personal information by law, because a court, the police or another law enforcement agency has asked us for it.

In accordance with GDPR, Marshall Assessment issue a 'change of learner personal details form' if any learner personal details change at any point during their course, we issue a form to overwrite their old information kept on their enrolment paperwork on file. The learner support team will also update the ILR database to ensure that all personal data is current and correct.

We process this information so that we can comply with various sector specific regulations. This allows us to comply with the Educations and Skills Funding Agency requirements to prove both the learner's identity and eligibility to receive government funds for their programme. Processing learner's personal information also allows us to improve the way we work, raise the quality of the teaching and learning experience while looking at trends in learner satisfaction and geographic area data. With this we can plan improvements for the future and better serve our customers.

Retention period

After completion of their End Point Assessment the learner's information is kept for a further 3 months. As n EPAO, we only need to keep learner's personal data for the purposes of administering the end of the apprenticeship plus 3 months post completion in order to send out certificates and final results. The duration of data storage is based upon our ability to request the necessary completion certificates from external agencies and the timelines they have for quality assurance purposes. Once this 3-month period is complete the personal information is deleted from our systems and hard copies are shredded. We will take anonymised statistical data from the information we hold but this will not be sufficient in nature to identify you any individuals or reveal any sensitive personal information about any of the learners.

Review

This policy and any underlining processes and procedures will be reviewed on a regular basis to ensure best practice and to take account of any changes in legislation. At a minimum, this review will be conducted on an annual basis.