ACADEMY
Online Learning Ltd

Data Protection Policy

Version 1.3

Edition Date: July 2023

Next Review Date: July 2024

1.0 Introduction

Academy Online Learning's (AOLL) processing of personal data complies with the eight enforceable principles of good practice. Data is:

- Processed fairly and lawfully
- Processed for limited or specified purposes
- Processed adequately, relevant and limited for use
- Accurate and where necessary up to date
- Not stored longer than necessary
- Processed in accordance with the data subject's rights
- Stored securely
- Not transferred to other countries outside the EEA without adequate protection.

2.0 Data Processing

Academy Online Learning stores sensitive personal information about its employees, prospective students, enrolled students, clients, trainers, suppliers, service users, professional advisors and consultants, complainants and enquirers; this may include:

- Personal details
- Family details
- Business activities of the person whose personal information we are processing

- Lifestyle and social circumstances
- Financial details
- Records of financial transactions with Academy Online Learning Ltd.
- Training details
- Education and employment details
- Goods and services

Sensitive classes of information are also processed and may include:

- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs
- Trade union membership

3.0 Purposes of Data Processing

Data is processed for the purposes of the educational requirements of students and maintenance of records required by educational bodies, such as

Access Validating Agencies. Employee data is necessary to ensure appropriate safeguarding and quality standards are maintained. Records of financial transactions are also stored.

We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act (DPA). What follows is a description of the types of organisations we may

need to share some of the personal information we process with for one or more reasons.

Where necessary or required we share information with:

- Business associates and other professional advisers
- Educators and examining bodies
- Current, past or prospective employers
- Family, associates and representatives of the person whose personal data we are processing
- Employment and recruitment agencies
- Financial organisations
- Credit reference agencies
- Debt collection and tracing agencies
- Suppliers and service providers;
- Persons making an enquiry or complaint
- Other companies in the same group
- Central Government

4.0 Accuracy of Information

There are checking processes in place to ensure important data is accurate and up to date. As part of the registration process students' Unique Learner Number (ULN) is obtained from the Learning Records Service and this ensures that the qualification data is associated with the correct individual learner and Personal Learner Record (PLR). In completing the registration form, learners also have the opportunity to correct any information that they may have recorded in error during enrolment.

5.0 Length of Storage

To ensure that data is not stored for longer than necessary, student user accounts are removed from the system on completion of their course and their work and learner records are archived and stored for no longer than two years this is to ensure that the work is available for scrutiny should this be required by the AVA or other relevant authorities.

In cases where learners fail to complete their course, they are entered for partial accreditation at the following moderation, their data is retained for two years as it is with those who complete with full accreditation.

6.0 The Rights of Data Subjects

All data subjects have the following rights:

- The right of access to a copy of the information comprised in their personal data
- The right to object to processing that is likely to cause or is causing damage or distress
- The right to prevent processing for direct marketing
- The right to object to decisions being taken by automated means
- The right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed

- The right to claim compensation for damages caused by a breach of the Act

Personal data is processed in accordance with the learner's right to

- Access: an individual can have access to personal data on request. The information must be requested in writing and the individual verified before disclosure. References given by AOLL to external organisations are exempt from access but the learner can ask for access to a reference AOLL has received. References produced for UCAS applications and HEI's are provided by tutors of AOLL.
- Accuracy: Individuals are able to ask for inaccurate personal data to be corrected and for out of date information to be updated
- To prevent processing likely to cause damage or distress: Individuals are able to ask for AOLL to stop processing information likely to cause unwarranted and substantial damage or distress; however, this does not apply to processing that is necessary for AOLL to fulfil its legal duties and commitments
- To prevent direct marketing: Individuals are able to opt-out of direct marketing and are only contacted for marketing purposes where there is prior agreement. Individual student email addresses are not available to other students.

7.0 Information Security

A number of measures are in place to ensure that information is secure from external attempts to obtain data:

- Only information that is necessary for the needs of the organisation is processed

- Members of the organisation are only given access to personal information necessary in the execution of their duties. For example, tutors do not have access to records of the financial transactions of their students
- Data is not passed to any third parties, except where necessary in delivery of services or where required by law
- Connections to the website and VLE are encrypted Secure Socket Layer connections to prevent sensitive information such as passwords, email and credit card details from hackers
- The server is protected by a firewall that only allows Secure Shell access from a single IP address
- Passwords are encrypted, salted and hashed to prevent 'brute force' attempts to guess passwords
- The website and VLE use secure, trusted software with regular security updates and these are implemented immediately on their release
- Personnel and contractors are required to encrypt removable media and mobile devices (e.g., laptops, tablet computers, mobile phones, USB drives) that are used for storing personal data.

8.0 Transmission of Data Outside the EEA

Academy Online Learning do not transmit any information to third parties outside the European Economic Area. If such a need arises in the future, steps will be taken to ensure that the data is secured in accordance with EEA rules.

There are sometimes occasions where information is transmitted to learners when they are outside the EEA. This only occurs in circumstances where either the learner has consented to or requested the information themselves or when it is necessary for performance of the contract between Academy Online Learning and the learner. An example of this would be a student accessing information from the Virtual Learning Environment from outside the EEA.