Aim2Learn Ltd Data Protection Policy

Aim2Learn Ltd is committed to the principles as codified in the ***Data Protection Act 1998*** in safeguarding the personal information of all learners and staff which is collected, stored or by necessity transferred (from one data base to another) electronically and /or in hard copy.

Data Protection and Protection of Personal data

Aim2Learn Ltd will ensure that all information acquired by parties in the delivery of contractual obligations will at all times comply with the provisions and obligations imposed by the Date Protection Act 1998 and the principles codified therein; together with any subsequent amendments/ updates regarding the storing and processing of personal data.

The process of personal data shall only be that necessary to the extent and in such a manner as is necessary for the provision of services or as is required by Law or any Regulatory Body.

Aim2Learn will ensure implementation of appropriate and technical [organisational] measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure.

Information obtained from learners is stored securely and only used for its original and intended purpose.

Security of stored Information

Aim2Learn ensures strict physical, electronic and administrative safeguards to protect users' personal information or the transfer of data from unauthorised or inappropriate access. Any person who accesses or transfers information without authorisation or for use other than its intended purpose will be subject to disciplinary action.
All Aim2Learn staff and learner users are made aware of Aim2Learn adherence to the principles stated in the ***Data Protection Act*** during Induction and staff training:

Data Protection Act 1998

Key Points

- All data must be obtained fairly and lawfully. For the purpose of learners on programme, most information will be collected during the registration period by designated personnel. Conditions must be satisfied for the processing of sensitive personal data that relate to ethnicity, political opinion, religion, trade union membership, health, sexuality or criminal record of the data subject.
- The Act covers personal data in both electronic form and manual form (e.g. paper files, card indices) if the data are held in a relevant, structured filing system.
- Personal data must be kept accurate and up to date and shall not be kept longer than necessary.
- Appropriate security measures must be taken against unlawful or unauthorised processing of personal data and against accidental loss of, or damage to, personal data. These include both technical measures, e.g. data encryption and the regular backing –up of data files and organisational measures, e.g. staff data protection training.
- Personal data shall not be transferred to a country outside the European Economic Area unless specific exemptions apply (consent) this includes the publication of personal data on the internet.

Data Subject Rights

The Act gives significant rights to individuals in respect of personal data held by them by data controllers. These include the rights:

- To make a subject access request – an individual is entitled to be supplied with a copy of all personal data held.
- To require the data controller to ensure that no significant decisions that affect them are based solely upon an automated decision-taking process.
- To prevent processing likely to cause damage or distress.
- To prevent processing for the purpose of direct marketing.
- To take action for compensation if they suffer damage by any contravention of the Act by the data controller.
- To take action to rectify, block, erase or destroy inaccurate data.

Data Protection Principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and kept up to date.
5. Personal data shall not be kept longer than is necessary to fulfil its purpose.
6. Personal data shall be processed in accordance with the rights of the data subject under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the E.U. unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Staff are required to sign this agreement and understanding of the above requirements.

Signed ..... Date .....