General Data Protection Regulation Policy

Purpose: To describe how A & S Transport Training Ltd aims to meet our legal requirements with respect to GDPR.

Scope: This policy applies to all areas of the company

Definitions:

- The 'company' refers to ‘A & S Transport Training’
- GDPR: General Data Protection Regulations

Responsibilities:

- The Director is responsible for the introduction and maintenance of this document.
- The ‘Data Protection Office’ (DPO – M. Mukerker) is responsible for managing the day-to-day requirements of this policy as detailed below.

Policy and Procedure

- Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy explains the duties and responsibilities of the company and it identifies the means by which the company will meet its legal obligations

Storage of information

- Information stored is collected from the individuals for attendance of their appropriate course. Information may include:
    - Name
    - Address
    - Postcode
    - Date of birth
    - Contact number
    - Email
    - Next of kin
    - Employer details (if applicable)

- The information ascertained in respect to the individual(s) or organisation(s), will be stored in accordance with the accredited / governing bodies criteria. The information will only be stored as reasonably practicable and required to allow A & S Transport Training to adhere to the criteria set. The company adhere to the criteria laid down by, with each dictating the length to which the information gathered must be held:
- Information will only be stored on the ‘company’ electronic devices i.e. laptop computers, which have been encrypted with passwords for the individual employees.

- Paperwork is stored and locked in the 'company' premises in storage devices. Storage cabinets and draws are used to store the information, which is locked when not in use. Designated members of staff are approved for access only.
- Information is only shared with the relevant awarding bodies.

Identifying the roles and minimising risk

- GDPR requires that everyone within the company understands the implications of GDPR and that roles and duties are assigned. The company is the data controller and has appointed a Data Protection Officer (DPO). It is the DPO's duty to undertake any information audit and to manage the information collected by the company, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information as necessary. These requirements will be included in the Job Description for the DPO

- GDPR requires care by everyone within the company, as a breach of the regulations could result in the company facing a fine from the Information Commissioner's Office (ICO) for the breach itself and possible compensation claims from any individual(s) adversely affected. Thus the handling of information is seen as a risk, both financially and to our reputation. Such risks can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments, minimising who holds data protected information and ensuring the company undertakes training in data protection awareness.

Data breaches

- One of the duties assigned to the DPO is the investigation of any data breaches. Personal data breaches should be reported to the DPO for investigation which must be undertaken within one month of the reported breach. Procedures are in place to detect, report and investigate any personal data breach. The ICO will also be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals. Where a breach is likely to result in a high risk to the rights and freedoms of these individuals, the DPO will also notify those concerned directly.

- It is unacceptable for non-authorised users to access our data systems using employees' log-in passwords or to use their equipment while logged on. It is unacceptable for employees, etc, to use IT in any way that may cause problems for the company.

Privacy Notices

- Being transparent and providing accessible information to individuals about how the company uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a company does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the company.

Data Protection Measures Implemented

- Use of a firewall is in place to secure Internet connection
- Secure settings of all devices / software are activated. Laptops, desktop computers, tablets and smartphones containing data have been password protected. Also details of the online accounts that are accessed, are also password-protected.
- Access to Data and Services is controlled with staff accounts have just enough access to software, settings, online services and device connectivity functions for them perform their role.
- Use of software is implemented to protect against viruses or other malware.
- Devices and software is kept up-to-date.

Information Audit

The Data Protection Officer must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the company will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the company undertakes a new activity.

Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place, these include:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

- The two enhancements of GDPR are that individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

- If a request is received to delete information, then the DPO must respond to this request within a month. The DPO has the delegated authority from the company to delete information.

- If a request is considered to be manifestly unfounded then the request may be refused or a charge may apply. The charge will be as detailed in the companies Freedom of Information Publication Scheme.

Children

We do not have any special requirements for children as we consider that there is no likelihood the company will be in a position where their data will require processing.

Summary

- The main actions arising from this policy are:
- The company must be registered with the ICO.
- A copy of this policy will be available on the company's website. The policy will be considered as a core policy for the company.
- The Job Description of the DPO will be amended to include additional responsibilities relating to data protection as and when required
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- Data Protection will be included on the company's general Risk Management Policy.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO. All employees are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the company.