DATA PROTECTION / GDPR POLICY

1. Statement of Intent

At Wildes Education we are serious about protecting and safely storing the personal data we collect from you. Wildes Education is the Data Controller when it comes to processing activities mentioned in this document. This means that Wildes Education decide why and how to collect and process your personal data. This policy applies to you if you are employed by Wildes Education, have enrolled on an apprenticeship programme provided by Wildes Education, or are registered as an employer for one of our learners.

2. The Aim of the Policy

The aim of the policy aims to explain how data should be protected and transferred in line with GDPR and the Data Protection Act 2018.

3. Six Data Protection Principles Under GDPR

Guidance states that data should be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. Individual Rights

Data subjects have the following rights regarding their personal data under the GDPR:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erase or "the right to be forgotten".
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

5. Definition of Sensitive Data

In addition to data which contains personal details about individuals is sensitive data. Information which contains racial or ethical origin, political views and religious beliefs and criminal convictions is extremely confidential. Confidential information about the company, its products and/or services, its customers and its suppliers is sensitive data.

6. Types of Data at Wildes Education

A large amount of data is stored electronically and paper-based. It is essential that this data is carefully protected and transferred securely in line with GDPR regulations and the Data Protection Act 2018.

The storing of data must adhere to the standards set out in line with GDPR. In particular it must be noted that personal data should not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of data protection.

7. Transferring of Data

The necessity of the transfer of any data should be considered prior to it taking place. Data should only be transferred when it is essential for the smooth operation of the company. The transferring of any sensitive data should always be authorised by the Managing Director prior to it happening.

8. Data Processing

All sensitive or confidential data should be encrypted, compressed and password protected before transmission. Appropriate technical and organisational measures are in place and action will be taken against any unauthorised or unlawful use or processing of personal data.

9. Memory Sticks/CD-ROMs

If data is to be transferred through memory sticks, CD-ROMs or similar formats, then the secure handling of these devices must be ensured. All documents on all devices should be password protected and encrypted. No such device should be sent through the open post, a courier service must always be used. The recipient should be clearly stated. If data is sent via a courier, the intended recipient must be made aware when to expect the data. The recipient must confirm safe receipt as soon as the data arrives. The sender is responsible for ensuring that the confirmation is received, and liaising with the courier service if there is any delay in the receipt of the data.

10. Data Disclosure

Legitimate personal data can be disclosed if:

- An individual has given consent for Wildes Education to correspond with a third party.
- In the legitimate interest of the individual to do their jobs.
- The organisation is legally bound to disclose information, for example to awarding bodies, funding organisations, etc.

The act permits disclosure of information in the following areas without consent:

- National security.
- Prevention of a crime.
- Collection of a tax assessment.
- Risk of harm to a third party.
- Life and death situations.

11. Retention and Disposal of Data

Where possible Wildes Education discourages excessive retention of personal data for longer than required. Once a staff member or learner has left it is unnecessary to keep personal information.

The Managing Director must be informed immediately if any confidential or sensitive data is missing. An immediate investigation will be launched to discover where the data has gone. If it is found that the data has been received by an unauthorised individual it must be determined whether that individual has accessed the data. If that individual has, and the data was correctly encrypted, compressed and password protected, it suggests that the individual has unlawfully accessed the data. In these situations, it might be appropriate to involve the police in the investigation.

The Managing Director will consider whether any individuals need to be informed about the data having gone missing, even if it is subsequently found. This might be necessary if there is a risk of personal data relating to individuals having been sent to the wrong person. If an employee has been negligent in transferring sensitive and confidential data this might be considered to be gross misconduct, which might result in summary dismissal. This is particularly likely to be the decision if:

- The likely employee did not encrypt, compress and password protect data.
- The employee transferred data using the open post and not a courier service.
- The employee transferred data without seeking the appropriate approvals.

12. Registration Number

Our Data Protection (ICO) Registration Number is ZA315928.