Policy 5

DATA PROTECTION AND CONFIDENTIALITY POLICY

M.E.A.T
(Ipswich) Limited

MEAT will endeavour to operate systems that are secure and respect the confidential nature of any information provided to its members of staff under the General Data Protection Regulations, requirement and BYOD (Bring your own device).

MEAT needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees, learners and other people the organisation has a relationship with or may need to contact.

This data protection policy ensures MEAT compiles with data protection law and follows good practice. Protects the rights of staff, learners, customers and partners. Is open about how it stores and process individuals' data and protects itself from the risks of a data breach.

The Data Protection Act 2018 describes how organisations including MEAT must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information is collected and used fairly, stored safely and not disclosed unlawfully.

MEAT will follow the Data Protection Acts seven important principles:

1. Be processed fairly, lawfully and transparent;
2. Be obtained only for specific, lawful purposes;
3. Personal Data will not be held for any longer than necessary;
4. Be accurate and keep up to date;
5. Processed in accordance with the rights of data subjects;
6. Steps to be taken to ensure personal data is processed and stored securely in agreement with Privacy Policy;
7. Accountability: In accordance with the Data Protection Act (EU 2016/679), we employ strict physical, electronic and administrative security measures to protect information from access by unauthorised persons and against unlawful processing, accidental loss, destruction and damage both on-line and off-line. The transmission of information via the internet is, however, not secure and therefore we cannot guarantee the security of data sent to us electronically. Any transmission of such data is therefore entirely at individuals own risk.

This applies to all data that the company holds relating to identifiable individuals this can include names of individual, postal addresses, email addresses, telephone numbers. This will help to protect MEAT from some security risks including, breaches of confidentiality, failing to offer choice and reputational damage.

Key staff and those how have access to data have key areas of responsibility; when data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it and kept in a locked drawer or cabinet, printouts should not be left where unauthorised people can see them (on printer) and data printouts should be shredded. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

New Employees

On appointment, new members of staff will be thoroughly briefed on the Company's policies and procedures. Training will be given to staff to ensure they protect and respect all information that may be deemed as confidential, from whatever source.

All Employees

Will ensure that all records or materials of a sensitive nature are stored in secure conditions.

Although information relating to learners is confidential, and kept in individual learners' files, relevant information relating to additional social and/or learning needs is provided to the appropriate people.

365 Microsoft data protected by Bit locker and Trend Micro Security.

Andrew MacDonald is the nominated General Data Protection person responsible for MEAT.

Signed:

JANE DALE

Managing Director.
Reviewed: April 2024
To be Reviewed: April 2025