DATA PROTECTION POLICY – CUSTOMER AND SUPPLIER DATA

Data Protection Policy - Customer and Supplier Data

As a Company, we are committed to safeguarding and preserving the privacy of our customer or supplier data. As an employee, you play a vital role in this process.

Anyone processing customer or supplier data must comply with the six enforceable principles of good practice. These provide that data must be:

a. Processed fairly, lawfully and transparently.

b. Collected for explicit, legitimate purposes and not processed further than stated to the subject.

c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. Accurate and up to date.

e. Not kept in an identifiable form for longer than necessary for the purpose.

f. Kept secure and monitored.

Data security

As an employee, you will maintain data security by protecting the confidentiality, integrity and availability of the data, defined as follows:

a. Confidentiality means that only people who are authorised to use the data can access it.

b. Integrity means that data should be accurate and suitable for the purpose for which it is processed.

c. Availability means that authorised users should be able to access the data if they need it for authorised purposes

Security procedures include but are not limited to:

e. ***Entry controls:*** Any stranger seen in entry-controlled areas (such as the Office or behind the Retail Counter) should be reported.

f. ***Secure lockable desks and cupboards:*** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

g. ***Methods of recording and disposal:*** You should not record any sensitive, financial or confidential information on paper. For instance, you will not record the bank or financial details of our suppliers or customers on paper. Instead, you must use the secure online payment system for recording such information. Paper documents should be shredded. Any digital storage devices should be physically destroyed when they are no longer required.

h. ***Equipment:*** Computer users must ensure that display screens/monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended, or otherwise apply the screen lockout function. Only portable media devices that have been encrypted may be used.

i. ***Training***: All staff must complete Data Protection (GDPR) training. Such training must be confirmed on staff appraisals and must be refreshed regularly.

Any data breach will be treated as gross misconduct and may result in dismissal.

Issued by: David McGuffie

Signed: 

Position: Director

Date: 21/03/2025

Review: 21/03/2026