

## 1. Agility Eco Data Protection Policy

### a. The Data Protection Act

We are committed to ensuring that we legally comply with the data protection principles, as laid down by the General Data Protection Regulation ("GDPR") and any implementing legislation under UK law, by:

- Ensuring that data is collected and used fairly and lawfully, with one or more lawful basis of processing
- Processing personal data only in order to meet our operational needs or fulfil legal requirements
- Taking steps to ensure that personal data is up to date and accurate
- Establishing appropriate retention periods for personal data
- Ensuring that data subjects are informed as to how we use their data, the rights they have in relation to that data and how to exercise those rights
- Ensuring that data subjects' rights can be appropriately exercised when this is requested
- Providing adequate security measures to protect personal data
- Providing that appropriate technological and organisational measures are used to protect personal data
- Ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- Ensuring that all staff are made aware of good practice in data protection
- Providing adequate training for all staff responsible for personal data
- Ensuring that everyone handling personal data knows where to find further guidance
- Ensuring that queries about data protection, internal and external to the organisation, is dealt with effectively and promptly
- Regularly reviewing data protection procedures and guidelines within the organisation

### b. Our data protection principles

The principles we apply to meet our commitments to these data protection principles are:

1. Personal data will be processed fairly, lawfully and transparently
2. Personal data will be obtained for one or more specified and lawful basis of processing, and will not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data will be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data will be accurate and, kept up to date
5. Personal data processed for any purpose or purposes will not be kept for longer than is necessary for that purpose or those purposes
6. Personal data will be processed in accordance with the rights of data subjects under the



#### GDPR

7. Appropriate technical and organisational measures will be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data will not be transferred to a country or territory outside the European Economic Area 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 or where adequate safeguards have been put in place

#### c. Staff obligations

As part of our commitment to our data protection principles, all staff are provided with a copy of this policy and receive adequate data protection training. All new staff are issued with the following reminder of the importance of data protection:

#### d. Data Protection

Protecting our assets by keeping our customer information safe is of utmost importance

Customer information is one of our most valuable assets. It enables us to achieve high levels of customer satisfaction to each customer.

Protecting the personal data of our customers is clearly not a debatable issue. As employees of AgilityEco we should all understand the importance of safeguarding customer information and also understand our legal and moral obligations around this information.

We need to work together to prevent any misuse of our information. We're helped by the standards set out in the GDPR. This law tells us to:

- > Use information fairly and lawfully
- > Keep information accurate and up to date
- > Observe data retention rules
- > Keep information securely at all times
- > Not disclose information externally without key controls

These points apply to all types of customer information from names and addresses though to billing details. However, financial details are much more valuable in the criminal world so additional precautions must be taken to protect this information, e.g. the extra questions we ask in the identification and verification of customers.

To illustrate the importance of this, there are some additional reminders from our own data protection guidelines:



- > Misusing information for personal gain is a criminal offence
- > Tampering with one customer account to benefit another is fraud
- > Buying and selling information is an illegal activity and will be treated accordingly

If any individual knowingly and/or deliberately breaches any of these rules, it will be classed as gross misconduct.

If you have any queries about the above or would like some help in this area please contact your manager. As a business, information is not something that we can, or want to, treat lightly.

9 April 2018

