



Greenwood Heating Ltd

“The Company”

Compliance Policy & Procedure Manual
Consumer Credit Activity

Key Contacts and Responsibilities

Company Name: Greenwood Heating Ltd

Company Address: 10 Greenwood Drive, Redhill, RH15PJ

Company Phone Number: 07547 372030

Approved Person: Darren Mackay

Direct Line of report if applicable:

Data Protection officer (DPO): Darren Mackay

The Money Laundering Reporting Officer (MLRO): Darren Mackay

Designated Complaints Handler: Darren Mackay

Document created by: Darren Mackay

Document owner: Darren Mackay

Document creation date: 3rd June 2021

Document review time scale: 6 Months.

Index

Page 2	Key Contacts & Responsibilities
Page 4	Anti-bribery & Corruption Policy
Page 8	Anti-Money Laundering Policy & Procedure
Page 12	Complaints Handling Policy & Procedure
Page 17	Conflicts of Interest Procedure & Reporting
Page 19	Vulnerable Customers Policy & Procedure
Page 28	Data Protection Policy
Page 36	Employee Initial Compliance Declaration
Page 37	Data Protection breach reporting
Page 38	Suspicious Activity reporting
Page 39	Business Gifts Reporting
Page 40	Conflicts of Interest Reporting
Page 41	Employee Initial Compliance declaration reporting
Page 42	Policy and Procedure Document review log.

Anti-bribery & Corruption Policy

What is Bribery?

Bribery is the accepting or giving of gifts, money, hospitality or other favours in return for providing something of value to the briber.

This is defined as giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person from having already done so i.e. seeking to influence a decision-maker by giving extra benefit to that decision-maker rather than by what can be legitimately offered as part of the tender process.

Who does this Policy cover?

The policy applies to all employees and sub-contractors alike.

What is the purpose of this Policy?

The purpose of this policy is to set out the rules that must be followed throughout the Company to ensure that no bribery or corruption occurs.

Scope

To comply with the legislation, we need to:

- Have adequate procedures in place to prevent bribery
- Have conducted a risk assessment to ensure that procedures are adequate to minimise the risk
- That any action taken is proportionate to the risk within the Company
- Top level commitment – demonstrate that all staff, sub-contractors and the key people with whom we do business with & for understand that we will not tolerate bribery
- Due diligence – know exactly whom we are dealing with and undertake checks before engaging others to represent us in business dealings. All due diligence checks of this nature will be recorded where appropriate
- Communicate policies & procedures to all employees and agents to enhance awareness and advise what is acceptable

- Monitoring & review – keep track of the risks faced particularly if entering a new market

Unacceptable behaviour

- Accepting any financial or other reward from any person in return for providing some favour
- Requesting a financial or other reward from any person in return for providing some favour
- Offering any financial or other reward from any person in return for providing some favour

Business Gifts

From time to time, customers, suppliers or other persons might offer a gift or reward to an employee. This could be anything from a small gift, money or something else of considerable value.

All gifts, however small, must be reported to an appropriate manager and recorded. No gifts with a value of more than £50 may be accepted.

If a gift is offered and then refused because of its value, this must be reported to an appropriate manager.

Hospitality

From time to time customers, suppliers or other persons may invite an employee to a hospitality event such as factory visits both in the UK and abroad, drinks and meal evenings, sports events like golf days.

All such invitations must be reported to an appropriate manager for authorisation prior to accepting the offer to attend the event. Such requests must be made via e-mail to support with auditing requirements.

Offering gifts & hospitality

The company may consider that from time to time, it is reasonable to offer small gifts or rewards to customers, suppliers or other persons. This may only be done when authorised by the Director.

Only when authorised by Director will any employee be allowed to offer gifts or rewards to customers, suppliers and other persons. In any such event a full record will be kept, providing details of the gifts/rewards and recipients by the company however small.

The company may occasionally hold hospitality events, primarily aimed at thanking customers, suppliers and other persons for their custom, loyalty, effectiveness or achievements. An employee must not organise any additional hospitality event without seeking authorisation from appropriate manager / owner.

Responsibilities of Staff

All members of staff are responsible for reporting to the Director all gifts & hospitality that is/are offered and/or received.

The Director is responsible for ensuring that all their responsible employees are aware of this policy and fully understand the rules in relation to the acceptance of gifts & hospitality.

Expenses

The Director must authorise all expenses claims from their employees and are expected to verify spending in this area by matching receipts.

Any item of expenditure that is not supported by a receipt or gives rise to concern that bribery may be taken place must be fully investigated at the earliest opportunity.

Attempts to bribe

Any employee who is concerned that he/she is potentially being bribed should report this matter to the manager or owner immediately.

Donations to organisations

From time to time, the company may make a charitable donation. These are managed by the firm's Director. No employee should make donations to charity on behalf of the Company unless authorised by firm's Director.

Under no circumstances are donations to be made to charities, political parties or other organisations with the intention of gaining personal or business advantage.

Raising concerns

If an employee is concerned that acts of bribery are occurring within the organisation they should inform the Director immediately.

If an employee is concerned that a supplier or company that we do business with may be corrupt, this should also be reported to the Director immediately.

Disciplinary action

All allegations of bribes being offered and/or received by an employee will be thoroughly investigated and dealt with using the company's disciplinary procedure.

The company will deem *proven* cases as Gross Misconduct and consequently disciplinary action, including summary dismissal could be considered.

Anti-Money Laundering Policy & Procedure

The Company will do all it can to prevent both it and staff being exposed to money laundering, to identify the potential areas where it may occur, and to comply with all legal and regulatory requirements, especially with regards to the reporting of actual or suspected cases.

1 Introduction

1.1 The Proceeds of Crime Act 2002, the Terrorism Act 2000 and the Money Laundering Regulations 2017 place obligations on the Company and its employees with respect to suspected money laundering.

2 Scope of the Policy

2.1 This Policy applies to all employees and aims to maintain the high standards of conduct which currently exist within the Company by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed (for example the reporting of suspicions of money laundering activity) to enable the Company to comply with its legal obligations.

2.2 This Policy sits alongside the Company's Fraud and Corruption & Whistle Blowing Policy.

2.3 Failure by a member of staff to comply with the procedures set out in this Policy may lead to disciplinary action being taken against them.

3 What is money laundering?

3.1 Money laundering is the term used for a number of offences involving the proceeds of crime or terrorism funds. The following acts constitute the act of money laundering:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327 of the Proceeds of Crime Act 2002);
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328); or
- Acquiring, using or possessing criminal property (section 329).

These are the primary money laundering offences, and are thus prohibited acts under the legislation. There are also two secondary offences: failure to disclose any of the three primary offences and tipping off. Tipping off is where someone informs a person or people who are, or who are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation.

Any member of staff could potentially be caught by the money laundering provisions, if they suspect money laundering and either become involved with it in some way and/or do nothing about it. This policy sets out how any concerns should be raised.

While the risk to the Company of contravening the legislation is low, it is important that all employees are familiar with their responsibilities: serious criminal sanctions may be imposed for breaches of the legislation. The key requirement on employees is to promptly report any suspected money laundering activity to the Money Laundering Reporting Officer.

4 Policy Statement

4.1 Our Policy is to do all we can to prevent, wherever possible, the Company and its staff being exposed to money laundering, to identify the potential areas where it may occur, and to comply with all legal and regulatory requirements, especially with regard to the reporting of the actual or suspected cases. We cannot stress too strongly, however, that it is every member of staff's responsibility to be vigilant.

5 The Money Laundering Reporting Officer (MLRO)

See "Main Contacts Form"

6 Procedures

Cash payments

6.1 No payment will be accepted in cash if it exceeds £5000

Reporting

6.2 Any employee who suspects money laundering activity must report their suspicion promptly to the MLRO, if you would prefer, you can discuss your suspicions with the MLRO.

6.3 The employee must follow any subsequent directions of the MLRO, and must not themselves make any further enquiries into the matter. They must not take any further steps in any related transaction without authorisation from the MLRO.

6.4 The employee must not disclose or otherwise indicate their suspicions to the person suspected of the money laundering. They must not discuss the matter with others or note on the file that a report has been made to the MLRO in case this results in the suspect becoming aware of the situation.

6.5 The MLRO must promptly evaluate any disclosure to determine whether it should be reported to the National Crime Agency (NCA).

6.6 The MLRO, if they so determine, promptly report the matter to NCA on their **standard report form** and in the prescribed manner.

6.7 The MLRO will commit a criminal offence if they know or suspect, or have reasonable grounds to do so, through a disclosure being made to them, that another person is engaged in money laundering and they do not disclose this as soon as practicable to the SOCA.

Identification of Clients

6.8 Where the Company is carrying out “relevant business” and, as part of this:

- (a) Forms an ongoing business relationship with a customer; or
- (b) Undertakes a one-off transaction involving payment by or to the customer of £10,000 or more; or
- (c) Undertakes a series of linked on-off transactions involving total payment by or to the client(s) of £10,000 or more; or
- (d) It is known or suspected that a one-off transaction (or a series of them) involves money laundering;

Then the **Customer Identification Procedure** (as set out below) must be followed before any business is undertaken for that customer.

6.9 Seek additional evidence of identity, for example:

- checking with the customer to confirm their UK address/proof of residency;
- Checking photographic ID;
- Seeking further evidence of personal identity and employment details/NI Number.

Record Keeping

6.10 Where “relevant business” is carried out then the customer identification evidence and details of the relevant transaction(s) for that customer must be retained for at least five years.

7 Guidance and Training

7.1 In support of the policy and procedure, the Company will:

- make all staff aware of the requirements and obligations placed on the Company and on themselves as individuals by the anti-money laundering legislation; and
- give targeted training to those most likely to encounter money laundering.

8 Further Information

8.1 Further information can be obtained from the MLRO and the following sources:

http://media.fshandbook.info/Handbook/FC1_FCA_20150427.pdf

http://media.fshandbook.info/Handbook/FC2_FCA_20150427.pdf

<http://www.nationalcrimeagency.gov.uk/publications/550-introduction-to-suspicious-activity-reports-sars-1/file>

<http://webarchive.nationalarchives.gov.uk/+http://www.hmrc.gov.uk/mlr/mlr8.htm>

Complaints Handling Policy and Procedure

Table of contents

1	REGULATORY REQUIREMENTS	12
2	PURPOSE	13
3	DEFINITION OF AN ELIGIBLE COMPLAINT	13
3.1	DEFINITION OF A COMPLAINT	13
3.2	ELIGIBLE COMPLAINANT	13
4	MEANS OF MAKING A COMPLAINT	14
5	TIME BARRED COMPLAINT	14
6	COMPLAINTS AWARENESS	14
7	COMPLAINTS ACKNOWLEDGEMENT	14
8	COMPLAINTS FORWARDING.....	14
9	COMPLAINTS INVESTIGATION	14
10	COMPLAINTS RESOLUTION.....	15
10.1	FINAL RESPONSE	15
10.2	SUMMARY RESOLUTION.....	15
11	GOVERNANCE	15
11.2	DESIGNATED COMPLAINTS HANDLER.....	16
11.3	ROOT CAUSE AND TREND ANALYSIS.....	16
11.5	INTERNAL AUDIT	16
12	RECORD KEEPING.....	16
12.1	RECORD STORAGE.....	16
12.2	RECORD RETENTION	16

1 REGULATORY REQUIREMENTS

- 1.1. The Financial Conduct Authority requires the Company to have internal procedures for the reasonable and prompt handling of complaints.
- 1.2. Principle 6 of the FCA’s Principles for Businesses requires the Company to treat customers fairly. TCF Outcome 6 requires the Company to ensure that customers do not experience any post-sale barriers such as experiencing difficulties in making complaints.

2 PURPOSE

- 2.1. The purpose of this document is to set out the policies and procedures that the Company must follow to ensure the reasonable and prompt handling of complaints.
- 2.2. This document is to be used by all of the Company staff who have interaction with customers and who can potentially receive customer complaints. This document provides a written framework to assist all relevant staff identify customer complaints and deal with such in accordance to the policies and procedures set out herein.

3 DEFINITION OF AN ELIGIBLE COMPLAINT

- 3.0. An eligible complaint is a complaint which should be handled in accordance to the policies and procedures set out in this document. There are two components that determine whether a complaint is an eligible complaint, namely (1) the complaint must satisfy the definition in paragraph 3.1.1. below and (2) the complaint must be made by an eligible complainant.

3.1 DEFINITION OF A COMPLAINT

- 3.1.1. An eligible complaint is defined by the FCA as *any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of a customer or potential customer about the provision of, or failure to provide, a financial service which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience and relates to an activity of the Company or any other organisation that the Company has some connection to in marketing or providing financial services or products.*
- 3.1.2. In other words, a complaint is any expression of dissatisfaction about the provision of the Company credit broking for boiler installation whether justified or not.

3.2 ELIGIBLE COMPLAINANT

- 3.2.1. In order for a complaint to be an eligible complaint it must be made by an eligible complainant. An eligible complainant can be a consumer (i.e. a natural person acting for purposes outside his trade, business or profession). Or a person acting on behalf of a corporate entity – proof of representative may be needed.
- 3.2.2. In light of this, all complaints that fall within the definition set out in paragraph 3.1.1. above that are made by the Company customers are eligible complaints that should be handled according to the policies and procedures set out in this document.

3.2.3. It is to be noted that reference to a customer includes a potential customer.

4 MEANS OF MAKING A COMPLAINT

A customer can make a complaint in line with the Company published consumer complaints processed available on the Company website.

5 TIME BARRED COMPLAINT

The Company will not accept complaints from customers after 6 years of works completed unless exceptional circumstances can be presented by the customer. Complaints presented more than 3 years after it is reasonable for the consumer to become aware of the issue and to have taken reasonable steps to reduce the impact of the problem, please be aware this does not include product failure where the guarantee provided by the manufacture exceeds the 6 years limit. In this case the complaint should be addressed directly to the manufacture.

6 COMPLAINTS AWARENESS

6.1. The Company makes consumers aware of its internal complaints procedure by publishing the same on its web site home page and finance page.

7 COMPLAINTS ACKNOWLEDGEMENT

7.1. The Company endeavours to send complainants a written acknowledgement of complaints within 14 working days.

8 COMPLAINTS FORWARDING

If we believe the complaint is in relation to a third for example a boiler manufacturer we will contact the customer to advise this and provide the best contact details to use. Where possible we will engage with the third party to support the resolution of any complaint.

9 COMPLAINTS INVESTIGATION

We endeavour to resolve all complaints fully within 4 weeks of being made aware. However this may not be possible depending on the circumstances of the complaint. If that is the case we will inform the customer in writing with an expected time scale.

10 COMPLAINTS RESOLUTION

10.1 FINAL RESPONSE

10.1.1. The Company will endeavour to issue a final written response to the complaint within 4 weeks.

10.1.2. The Company's final response will either:

- 8.1.2.1. Accept the complaint and, where appropriate, offer redress or remedial action;
- 8.1.2.2. Offer redress or remedial action without accepting the complaint; or
- 8.1.2.3. Reject the complaint and give reasons for doing so.

10.1.3. If the Company is not in a position to issue a final response within 8 weeks, the complainant will be provided with a written response explaining why the Company is not in a position to issue a final response and set out the date by which the Company expects to be able to issue one. At this point, complainants have the right to refer their complaint to the Financial Ombudsman Service should they choose to not wait beyond the 8-week timescale for the Company to issue a final response.

10.2 SUMMARY RESOLUTION

10.2.1. The Company does not provide complainants with a written complaints' acknowledgement and a written final response where the Company resolves the complaint by close of business on the third business day following the day on which the complaint is received. The Company instead provides complainants with a summary resolution communication. A summary resolution communication sets out:

- 8.2.1.1. The fact that a complaint has been made;
- 8.2.1.2. Informs the complainant that the complaint has now been resolved; and
- 8.2.1.3. Sets out the complainant's right to refer the complaint to the Financial Ombudsman Service should they subsequently be dissatisfied with the resolution and sets out the contact details of the Financial Ombudsman Service including its website.

11 GOVERNANCE

11.1 DESIGNATED COMPLAINTS HANDLER

On behalf of the business the above named will respond to all communications with both the consumer and any regulated body including financial ombudsmen service were required. From time to time it may be in the customer's best interest for another member of our team to make contact during the complaint process. In this case we will outline to the customer why this person is making contact the position they hold within our business.

11.2 ROOT CAUSE AND TREND ANALYSIS

Will regularly review the complaints we receive and ensure we are identify and trends or indicators that will allow us to improve the service and protection we provide customers. These reviews will be recorded.

11.3 INTERNAL AUDIT

During our half yearly reviews this policy and our complaints process will be assessed to ensure that they are in line with the needs of our customers and the operating standards of our industry.

12 RECORD KEEPING

12.1 RECORD STORAGE

All complaints, review and responses will be kept within our in computer systems for a reasonable time scale.

12.2 RECORD RETENTION

Records will be keep and accessible including reporting options for a mimum of 6 years. Should any date be relevant to the ongoing support of our customers it may be kept for longer, in this case the reason for retaining the information will be given.

Conflicts of Interest Procedure & Reporting

Procedure

Actual, potential and perceived conflicts of interest are to be reported, managed and effectively avoided. If there is any doubt as to whether a conflict of interest exists, it is best to assume that it does and act accordingly. It is the responsibility of all staff to report any potential conflicts of interest to their Line Manager or the Company's Director. (See Organisational Structure). The management team can then resolve to manage the issue in a timely manner to avoid further conflict

1. Gifts & Hospitality

Any offers of gifts or hospitality must be recorded on the Gifts & Hospitality Register. This will be reviewed by the Company director.

Entertainment given or received in the normal of business e.g. lunches, business travel, does not require approval or notification.

All gifts to be given or received, in the course of the Company's regulated business with a value of £50 or more must be entered onto the gifts register held by the Company Director.

Employees and their family members may not accept or give gifts or special favours above £100. However, where a series of gifts, from the same individual and in succession such that the gifts represent a single inducement, represents a value of £100 or greater, no further gifts will be allowed.

Regardless of value, employees must ensure that no gift or series of gifts creates a conflict or influences the level of service provided to the customer. Cash gifts are never appropriate and must not be offered or accepted.

The Company Director maintains a register of all gifts and entertainment given or received. The Company Director will review the register on periodic basis to ensure that there is no evidence of any undue influence being created by any gifts or series of gifts. Employees may be asked to provide additional information as a result of this review.

Employees should use their judgement when offering or accepting gifts to ensure that they are unlikely to be so influenced that it may cause them to breach any duties that they have under the FCA requirements or customer agreements.

In considering whether a gift or form of entertainment is excessive, the Company Director will bear in mind the client relationship and whether it could be regarded as an improper inducement, either by the employer of the recipient or donor or by the supervisory authorities.

When in doubt whether a gift requires approval, all employees are advised to report the item for approval or consult the Company Director.

The Company will take the following action in relation to bribery and corruption:

- Any suspicions of bribery, corruption or unusual business practices should be reported to the Company's Legal Director.
- Where actual Bribery has taken place, this is a criminal offence and will be reported to the police.
- Any allegations of Bribery will be thoroughly investigated and may result in disciplinary action in accordance with the Company's Disciplinary Policy.

2. Promotions & Appraisals

Promotions and Appraisals are factually based and take into account staff behaviour and performance in their current job roles. Staff are promoted objectively, based not only on their performance but their behaviour.

3. Fraternalisation

All staff are discouraged from entering into relationships with members of staff who may or could be under their charge. This presents a clear conflict of interest as this may promote favouritism. The customer may be affected as that member of staff may be treated more leniently for breaching any of FCA Principles.

Reporting

All members of staff will report any issues that may amount to conflicts of interest to his Line Manager who will in turn report to the Company Director. The Company Director will then create a report (see our Register of Interests Reporting Form) on the issue and act in a timely manner to prevent further conflict.

Vulnerable Customers Policy and Procedure

Table of contents

1	PURPOSE.....	19
2	REGULATORY REQUIREMENTS	20
3	APPLICATION.....	20
3.1	DEFINITION OF VULNERABLE CUSTOMERS.....	20
3.2	ACTUAL AND POTENTIAL VULNERABILITY	21
4	IDENTIFYING VULNERABLE CUSTOMERS.....	21
5	DEALING WITH THIRD PARTIES REPRESENTATIVES	25
6	MAKING ADJUSTMENTS TO SERVICE DELIVERY	25
7	MAKING RECORDS	25
7.1	ORDINARY RECORDS	25
7.2	SPECIAL CATEGORY PERSONAL DATA	26
8	OBTAINING EVIDENCE	26
8.1	CIRCUMSTANCES WHERE EVIDENCE IS REQUIRED	26
8.2	TIMESCALE TO OBTAIN EVIDENCE	26
8.3	INTERNAL INVESTIGATION.....	26
10	MAKING REFERRALS TO THIRD-PARTY SUPPORT PROVIDERS.....	26
11	GOVERNANCE	15
11.2	INTERNAL AUDIT	16
12	RECORD KEEPING.....	16
12.1	RECORD STORAGE.....	16
12.2	RECORD RETENTION	16

1 PURPOSE

- 1.1. The purpose of this document is to set out the policies and procedures that the Company has in place to ensure the fair and appropriate treatment of customers, who the Company understands or reasonably suspects to be vulnerable or particularly vulnerable.
- 1.2. This document is for the use of the Company's staff who interact with customers in any capacity or otherwise operate in a capacity where they can be reasonably aware of information that indicates a customer is vulnerable or particularly vulnerable, and

provides a documented framework to promote the consistent fair treatment of customers who are vulnerable or particularly vulnerable.

2 REGULATORY REQUIREMENTS

2.1. Consumers are placed at the centre of the FCA's regulatory regime and their protection is one of the FCA's operational objectives. The FCA advances its consumer protection objective through its high-level principles, as set out in the Principles for Businesses module of the FCA Handbook, and specific conduct rules that apply to the Company's regulated activities.

2.2. The Principles for Businesses that underpin the fair treatment of vulnerable customers are as follows:

2.2.1. Principle 2 - A firm must conduct its business with due skill, care and diligence;

2.2.2. Principle 3 - A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems;

2.2.3. Principle 6 - A firm must pay due regard to the interests of its customers and treat them fairly; and

2.2.4. Principle 7 - A firm must pay due regard to the information needs of its clients, and communicate information to them in a way which is clear, fair and not misleading.

2.2.5. Principle 6 underpins the Firm's obligation to ensure the fair treatment of vulnerable customers in that the fair treatment of customers depend, in part, on the characteristics of the customers concerned therefore, to pay due regard to their interests and treat them fairly, the Firm must understand what makes such customers vulnerable, understand their needs, and ensure the finance options for boiler installation it provides supports the fair treatment of vulnerable customers.

2.3. The Principles of Businesses are supplemented by conduct rules which require the Firm to establish and implement clear, effective and appropriate policies and procedures for the fair and appropriate treatment of customers, who the firm understands or reasonably suspects to be vulnerable or particularly vulnerable.

3 APPLICATION

3.1 DEFINITION OF VULNERABLE CUSTOMERS

3.1.1. The FCA defines a vulnerable consumer as ‘someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a Company is not acting with appropriate levels of care’.

3.2 ACTUAL AND POTENTIAL VULNERABILITY

3.2.1. The policies and procedures set out in this document ensure that the Company identifies and appropriately treats consumers who are *actually* vulnerable and consumers who are *potentially* vulnerable.

3.2.2. A customer that is actually vulnerable is one where, due to their current personal circumstances meets the definition in paragraph 3.1.1. The range of actual vulnerabilities in the Company’s target market or customer base are as follows:

1. Someone without the mental capacity to fully understand the agreement they are entering.
2. Someone who may struggle to understand the long term implications of the agreement they are entering into.
3. Someone who struggles with any form of communication, for example hearing or reading.
4. Someone who declares a poor understanding of credit or credit scoring.
5. Someone where English may not be the first language.
6. A customer who may demonstrate or declare a mental health issue or concern
7. A customer who may have encountered a negative life event that could affect understanding or decision making.

3.2.3.1. Details out lined in our customer facing vulnerable customer’s policy.

3.2.3. A customer that is potentially vulnerable is one that, although not currently vulnerable, may be more susceptible to harm in comparison to other customers due to certain characteristics. The range of potential vulnerabilities in the Firm’s target market or customer base are as follows:

4 IDENTIFYING VULNERABLE CUSTOMERS

The characteristics that we use to identify potentially vulnerable customers can be found on our customer facing vulnerable customer policies.

Treating customers fairly policy

Introduction

The Financial Conduct Authority's (FCA) Treating Customers Fairly (TCF) Principle 6 requires a firm to pay due regard to the interests of its clients and treat them fairly. We are fully committed to TCF and this Policy has been designed to demonstrate the application of TCF during our day to day activities.

TCF is embedded throughout the FCA's Handbook and the FCA's six core consumer outcomes are embedded in our firm. These are:

- Consumers can be confident they are dealing with firms where TCF is central to the corporate culture.
- Products and services marketed and sold in the retail market are designed to meet the needs of identified consumer groups and targeted accordingly.
- Consumers are provided with clear information and are kept appropriately informed before, during and after the point of sale.
- Where consumers receive advice, the advice is suitable and takes account of their circumstances.
- Consumers are provided with products that perform as firms have led them to expect and the associated service is both of an acceptable standard and as they have been led to expect.
- Consumers do not face unreasonable post-sale barriers imposed by firms to change product, switch provider, submit a claim or make a complaint.

Our TCF Mission Statement

We will act with integrity in everything we do and put our customers at the heart of our business.

Our TCF Principles

- Customers will be provided with clear information and kept appropriately informed before, during and after the point of sale.

- If we give advice to our customers, the advice will be suitable and take account of their circumstances.
- Our level of service and product performance will meet the expectations of our customers as far as reasonably possible.
- We will ensure that there is no barrier for customers to express their requests, concerns or complaints, and will always be responsive to them.
- Products and services will be designed to meet the needs of our customers.

Assessing and implementing our TCF Principles

Marketing

All our financial promotions and marketing materials are reviewed to ensure that they are appropriate for our target audience and are presented in a clear, fair and not misleading manner.

Sales, Advice, Management

When providing advice, our advisers obtain a detailed understanding of the customer's needs so that our recommendations are suitable. We ensure that our customers understand the risks involved with any service or product offered and are aware of all fees and charges.

Post-Sale Information and Support

We strive to keep our customers informed pre, during and post contract. Appropriate records are held and can be provided as required on an ongoing basis. We have appropriate capacity for storing and processing information to ensure continuous support. We have no post-sale barriers in place which restrict customers' access.

Policies and Procedures

We have policies and procedures that are relevant to the fair treatment of our customers and which also meet FCA requirements. These are (this not an exhaustive list):

- Conflicts of Interest Policy
- Data Protection Policy
- Vulnerable Customers Policy
- Training and Competence Policy

- Financial Crime including Bribery & Corruption & Money Laundering
- Complaint Handling Procedures
- Financial Promotions Procedures

Management Information (MI)

We produce MI to assess our performance against the TCF principles. We ensure that MI is accurate, timely, consistent and relevant to assist the business to make informed decisions in the best interests of our customers. We produce MI reports which are reviewed regularly by senior managers, directors and board members in various meetings.

Awareness/Training

We ensure that all advisers and staff are familiar with the TCF Principle and its outcomes. In addition, where applicable, advisers and staff are trained to advise on and adequately explain our products and services. We make sure that all advisers and staff achieve the necessary qualifications and training to carry out their role to the required competence level. We undertake regular monitoring and assessment of our advisers and staff so that we can ensure their competence.

Compliance

We maintain a Compliance Monitoring Programme which clearly lists areas of responsibilities and the frequency of checks required.

We have a compliance team who is independent and regularly monitors all key areas of regulatory compliance including TCF.

Every year we carry out a TCF Self-Assessment to measure our performance and which highlights areas of improvement

Remuneration

We operate a remuneration model that does not reward on sales performance only, to mitigate sales bias. We reward non-sales staff in a way which does not negatively impact on the treatment of our customers. All staff contribute to the firm's overall target. The sale of finance is not incentivised.

Complaints

Our goal is to provide excellent customer service and complaint handling plays a major part in our TCF policy. We deal with customer complaints fairly and objectively and attempt to put things right as quickly as possible, in accordance with the requirements of the FCA Dispute & Resolution Handbook.

All complaints are recorded and monitored, and a root cause analysis performed. All are reported as MI and analysed in senior management meetings.

Conclusion

We encourage a culture of personal responsibility and impress upon all involved with our firm that a good culture is central to the economic health of our firm. We strive to build a strong conduct culture which builds both customer trust and inspires employees. Getting the culture and conduct right is in the interests of our economic strength and our shareholders.

We frequently review our policies, procedures and practices to ensure that TCF remains central to our firm.

We ask our clients to provide us feedback, sometimes formally through customer surveys, so which enables us to improve our service. The information we gather from our customers is reported in our MI and reviewed by senior managers, directors and board members to help shape any strategic decisions.

5 DEALING WITH THIRD PARTIES REPRESENTATIVES

We are willing to deal with third parties dealing with the concerns of a vulnerable customers. To protect that customer we may require evidence that the third party is authorised or legally in a position to act on our customers behalf.

6 MAKING ADJUSTMENTS TO SERVICE DELIVERY

Depending on the needs of the customer we endive to make all reasonable changes to the way that we work to ensure all customers are protected and provided the support they need. If we feel that we are unable to make the needed changes for example for health and safety reasons we will outline our approach to the customer and their 3rd party where relevant.

7 MAKING RECORDS

7.1 ORDINARY RECORDS

If we make any changes to the way that we operate with a customer details will be recorded within the customer's account held by ourselves. This information will be kept for the duration of the customer account.

7.2 SPECIAL CATEGORY PERSONAL DATA

No special category data will be recorded or stored.

8 OBTAINING EVIDENCE

8.1 CIRCUMSTANCES WHERE EVIDENCE IS REQUIRED

Where we may need to request evidence to support the position of a vulnerable customer this will be requested in writing clearly outlining what we request and for what reason.

8.2 TIMESCALE TO OBTAIN EVIDENCE

It will be the customer's reasonability to provide any requested evidence. We will not commence works until all parties are happy. This means that any delay in returning information may result in a delay in the commencement of works.

8.3 INTERNAL INVESTIGATION

When deciding if works should continue for a person who is vulnerable the decision will be made internal via consultation with our management team. We may from time to time engage with third parties for example the FCA or Hitachi our lender to ensure we are making a decision that has the customer's best interest at heart. In this case minutes will be taken and stored with our customer records.

9 MAKING REFERRALS TO THIRD-PARTY SUPPORT PROVIDERS

Please see our customer facing vulnerable customer's policy's to understand who we may refer vulnerable customers to if we feel it is the right action to take.

10 GOVERNANCE

This policy and procedure will be reviewed every 6 months to ensure it continues to meeting the required standards of our customers, regulatory bodies and industry standards.

11 RECORD KEEPING

11.1 RECORD STORAGE

All information in relation to vulnerable customers will be held with the relevant customer account.

11.2 RECORD RETENTION

Records will be kept and accessible including reporting options for a minimum of 6 years. Should any data be relevant to the ongoing support of our customers it may be kept for longer, in this case the reason for retaining the information will be given.

Data protection policy

1 Context and overview

Introduction

The Company needs to gather and use certain information about individuals.

Individuals can include customers, suppliers, business contacts, employees and other people the Company has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures that we:

- Comply with data protection law and follow good practice;
- Protect the rights of staff, customers and partners;
- Are open about how we store and process individuals' personal data;
- Protect the Company from the risks of a data breach

Data protection law

The General Data Protection Regulation describes how we 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 must be collected and used fairly, stored safely and not disclosed unlawfully.

The General Data Protection Regulation is underpinned by six important principles. These say that personal data must:

1. Be processed fairly, lawfully and in a transparent manner;
2. Be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Be accurate and, where necessary, kept up to date;
5. Be kept for no longer than is necessary for the purposes for which the personal data is processed; and
6. Be processed in a way that ensures appropriate security of the personal data.

2 People, risks and responsibilities

This policy applies to:

- All staff and volunteers
- All contractors, suppliers and other people working on behalf the Company

It applies to any information which we hold relating to an individual from which an individual can, directly or indirectly, be identified. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Reference numbers

Data protection risks

This policy helps to protect the Company from some very real data protection risks, including:

- Breaches of confidentiality.** For example, information being given out inappropriately.
- Excess information collection.** For, example collecting more personal information than is necessary for the Company to provide the service.
- Failing to offer choice.** For example, all individuals should be free to choose how the company uses data relating to them.
- Out of date.** For example, storing out of date and inaccurate information.
- Data retention.** For example, keeping personal information indefinitely when no longer in use.
- Reputational damage.** For example, the Company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who handles personal information within the Company has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, the following people have key areas of responsibility:

The **Company Directors** is ultimately responsible for ensuring that the Company meets its legal obligations.

The **Company Director** is responsible for:

- o Keeping the board updated about data protection responsibilities, risks and issues.
- o Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- o Arranging data protection training and advice for the people covered by this policy.
- o Handling data protection questions from staff and anyone else covered by this policy.
- o Dealing with requests from individuals to see the data the Company holds about them (also called 'subject access requests').
- o Dealing with requests from individuals who want to exercise their rights under GDPR (e.g. request erasure of their personal information)
- o Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- o Carrying out data protection risk assessments
- o Carrying out internal data protection audits
- o Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- o Performing regular checks and scans to ensure that security hardware and software is functioning properly.
- o Evaluating any third-party services the Company is considering using to store or process data. For instance, cloud computing services.
- o Approving any data protection statements attached to communications such as emails and letters.
- o Addressing any data protection queries from journalists or media outlets like newspapers.
- o Where necessary, working with other staff to ensure marketing initiatives abide by the data protection principles.

3 General staff guidelines

The only people able to access data covered by this policy should be those who **need it for their work**.

Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.

The Company will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, **strong passwords must be used** and they should never be shared.

Personal data **should not be disclosed** to unauthorised people, either within the company or externally.

Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees **should request help** from their line manager or the Compliance Officer if they are unsure about any aspect of data protection.

4 Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Company Director.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. For example visitors to the business both general public, delivery operatives, manufacture representatives and cleaning staff.

No Data should be left of desks or in common areas.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.

Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.

Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.

Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.

Servers containing personal data should be **sited in a secure location**, away from general office space.

Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.

All servers and computers containing data should be protected by **approved security software and a firewall**.

5 Data use

Personal data is of no value to the Company unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended. Ctrl + Alt + Del before you leave your seat.

Personal data **should not be shared informally**. It should never be sent by email, as this form of communication is not secure.

Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.

Personal data should **only be transferred outside of the European Economic Area** if the receiving Company has adequate data security measures.

Employees **should not save copies of personal data to their own computers**. Always access and update the central copy of any data.

6 Data accuracy

The law requires us to take reasonable steps to ensure data is kept accurate

and up to date.

It is the responsibility of all employees who work with data to take steps to ensure it is kept accurate and up to date.

Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.

Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.

The Company will make it **easy for data subjects to update the information** it holds about them. For instance, via the Company website.

Data should be **updated immediately inaccuracies are discovered**. For example, if a customer can no longer be reached on his stored telephone number, it should be removed from the database.

It is the Company Directors responsibility to ensure **marketing databases are checked against industry suppression registers** every six months.

7 Individuals' rights

All individuals who are the subject of personal data held by the Company are entitled to:

1. Obtain confirmation about **what information** we hold about them and to **access copies** of that information.
2. Request the **correction** of inaccurate personal information.
3. Request the **erasure** of their personal information.
4. **Restrict** how their personal information is used.
5. Receive their personal information in a **legible** and **transferable** format. For example, in an Excel format.
6. **Stop** the use of their personal data.
7. **Object** to their personal information being used for an automatic decision.
8. **Be informed** about why their personal information is being collected and how it will be used.

The Company must make it easy for individuals to exercise their rights in relation to their personal information. Where an individual makes any of the above requests we must comply within one month.

The Company cannot charge a fee to an individual for exercising his rights unless the request from the individual is excessive. For example, because it is a repetitive request that has previously been complied with.

Any charge should be limited to the administrative cost of complying with the

request.

The Company Director will always verify the identity of anyone making a request to exercise his individual rights before auctioning the request.

8 Disclosing data for other reasons

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the individual.

Under these circumstances, the Company will disclose the requested data. However, the Company Director will ensure the request is legitimate, seeking assistance from the board and from the Company legal advisers where necessary.

9 Providing information

The Company aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used

- Who their data is being shared with

- How long their data will be stored

- How to exercise their rights

- How to lodge a complaint with the Information Commissioner's Office

To comply with the above, the Company has a privacy statement, which sets out how data relating to individuals is used by the Company.

This is available on request. A version of this is also available on our website

Employee Initial Compliance Declaration

I hereby confirm that:

1	I will conduct myself in conformity with, and so as to result in the Company complying with, the rules and regulations made from time to time by the FCA (the 'Rules') as if they were directly binding on me so far as it is reasonably in my power to do so.	Yes <input type="checkbox"/> No <input type="checkbox"/>
2	I will report any known breaches of the Rules to the Company Director as soon as I become aware of such a breach.	Yes <input type="checkbox"/> No <input type="checkbox"/>
3	I will report any complaints, either written or oral, received from clients to the Company Director as soon as they are received.	Yes <input type="checkbox"/> No <input type="checkbox"/>
4	I will read and comply with the Company's current Compliance manual and relevant Policies and Procedures which I have been made aware and I will consult the Company Director or my line manager if I have any questions or concerns regarding of the issues set out therein.	Yes <input type="checkbox"/> No <input type="checkbox"/>
5	I have read and understood the Company's Money Laundering Awareness Policy and Procedures and understand my obligation to report any suspicions of money laundering to the Money Laundering Reporting Officer	Yes <input type="checkbox"/> No <input type="checkbox"/>
6	I am aware and will comply with the Company policy regarding gifts and inducements.	Yes <input type="checkbox"/> No <input type="checkbox"/>
7	I have notified all my current outside interests to the Company Director and understand and will comply with the Company requirement to any changes to my outside interests as soon as practicable.	Yes <input type="checkbox"/> No <input type="checkbox"/>
8	I will consider my training and competency requirements in respect of my roles and duties. I will raise any concerns or requirements in respect of ongoing training with my line manager and ensure these requirements are addressed to my satisfaction so that I can consider that I am adequately trained and competent to carry out my role.	Yes <input type="checkbox"/> No <input type="checkbox"/>
9	I understand that this confirmation forms part of my contract of employment and that any breach of it may result in my being subject to the Company's disciplinary proceedings.	Yes <input type="checkbox"/> No <input type="checkbox"/>

END

Data Protection Breach Report Form

DATE OF BREACH	DETAILS OF BREACH	INDIVIDUALS AFFECTED (E.G. CUSTOMERS, STAFF)	APPROX. NUMBER OF INDIVIDUALS AFFECTED	APPROX. NUMBER OF PERSONAL DATA RECORDS CONCERNED	TYPE OF DATA AT RISK	POTENTIAL CONSEQUENCE OF BREACH	MITIGATION ACTION	REPORTED TO ICO	DATE REPORTED TO ICO	COMMUNICATED TO DATA SUBJECTS	SIGNATURE

Please print this page and store separately

Suspicious Activity Reporting Form

Incident number	Incident date	Details of activity	Investigated by	Outcome	Reported to police, FCA etc (if applicable)	Date reported (if applicable)

Please print this page and store separately

Business Gifts – reporting log (when in excess of £50)

DATE	GIFTED	RECIPIENT	VALUE	MANAGER SIGNATURE

Please print this page and store separately

Conflicts of interest reporting log

DATE	STAFF MEMBER	DETAILS OF CONFLICT	BUSINESS CRITICAL	MANAGER SIGNATURE

Please print this page and store separately

