Anti Fraud Policy (including bribery, corruption, tax-evasion and money-laundering)

INTRODUCTION

Restore Compliance provides Building Control and Consultancy Services and is fully committed to the highest standards of conducts from both employees and our approved supply chain. As a consequence, it is essential that all associated with the business are fully aware of the risk of fraud, theft, corruption, money-laundering, bribery, tax evasion and any other activities that could be deemed dishonest.

Restore Compliance has a 'zero tolerance' to any activities that could be deemed dishonest.

SCOPE AND OBJECTIVES OF THE POLICY

This policy is based around a centralised key objective to ensure that any form of dishonest activity is seen as unacceptable by each member of the Restore Compliance team and any countermeasures are fully supported and engaged with. To achieve this objective Restore Compliance will ensure any dishonest activity is addressed fairly and in a timely manner, company assets and reputation are always protected and to have an open reporting channel that fully supports any employees who raises concerns. This policy has been created in compliance with the Anti Bribery Act 2010.

DEFINITIONS

Fraud: An array of irregularities and illegal acts characterised by intentional deception with intent to make a gain or to cause a loss, or to expose another to a risk of loss. It can be perpetrated for the benefit of or to the detriment of Restore Compliance and by persons outside as well as inside the company.

Bribery: An inducement or reward offered, promised, received or provided to gain personal, commercial, regulatory or contractual advantage and such advantage leads to the improper performance of a relevant function or activity.

The Company will not:

- Make contributions of any kind with the purpose of gaining any commercial advantage.
- Provide gifts or hospitality with the intention of persuading anyone to act improperly, or to influence a public official in the performance of their duties.
- Make, or accept, "kickbacks" of any kind.

The Company will:

- Keep appropriate internal records that will evidence the business reason for making any payments to third parties.
- Encourage employees to raise concerns about any issue or suspicion of malpractice at the earliest possible stage.
- See that anyone raising a concern about bribery will not suffer any detriment as a result, even if they turn out to be mistaken.

Employees must not:

- Accept any financial or other reward from any person in return for providing some favour.
- Request a financial or other reward from any person in return for providing some favour.
- Offer any financial or other reward from any person in return for providing some favour.

Corruption: The offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions of an Restore Compliance employee or appointed contractor.

Tax Evasion: Criminal conduct which involves individuals or businesses paying too little tax or wrongly claiming tax repayments by acting dishonestly. It is an offence to dishonestly "take steps with a view to" or "be knowingly concerned in" the evasion of the tax. For these offences to be committed it is not necessary that any tax actually be successfully evaded. It is now also an offence for the company to fail to take appropriate steps to prevent an associated person criminally facilitating the evasion of a tax, and this will be the case whether the tax evaded is owed in the UK or in a foreign country. Examples:

- Knowingly entering false or misleading information in relation to the employment of an individual to facilitate the underpayment of income tax
- Knowingly processing invoice payments or raise debt to facilitate the underpayment of tax
- Knowingly processing documents for services supplied to the company as being outside the scope of VAT, when they should be in scope
- Knowingly helping an overseas contractor to avoid overseas tax on payments they make to the company
- Knowingly processing a payment to an employee / contractor as an expense rather than another type of payment which would be subject to tax.

Money Laundering: The term used to describe a number of offences involving the proceeds of crime or terrorist funds. It is a criminal offence to:

- Conceal, disguise, convert, transfer or remove criminal property from the United Kingdom
- Enter into or become concerned in an arrangement which an individual knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- Acquire, use or possess criminal property
- Fail to disclose one of the principal offences listed above, where there are reasonable grounds for knowing or suspecting the money was a proceed of crime
- Tell someone that you are going to make a report or tell someone that they are being investigated (tipping-off)
- Falsify, destroy, dispose of, conceal any document which is relevant to an investigation, or allow this to happen.

ACTIONS TO BE TAKEN IN THE EVENT OF SUSPECTED ACTIVITIES

If potentially suspicious activity within the company has been identified:

Do:

- Write down your concerns immediately – make a note of all relevant details such as what was said in phone or other conversations, the date, the time and the names of anyone involved.
- Consider the possible risks and outcomes of any action you take.

- Make sure your suspicion is supported by facts.

Do not:

- Become a private detective and personally conduct an investigation.
- Do not approach the person involved (this may lead to them destroying evidence).
- Do not discuss your suspicions with anyone other than the person to whom you should make the initial report unless asked to do so as part of a formal investigation.

Remember:

- You may be mistaken or there may be an innocent or good explanation.
- The process may be complex, and the situation may lead to a period of disquiet or distrust in the organisation despite you having acted in good faith.

REPORTING AND INVESTIGATING

Should a member of staff identify potential suspicious activities that they wish to report, any concerns or allegations they should be directed to line management or a Director. Confidential reporting can be carried out in line with the whistleblowing process. in the case of money laundering the, the finance Lead must be included within any investigatory meetings.

In addition to activating the internal investigation procedures the Directors will also notify the police authorisation as and when appropriate.

SECURING EVIDENCE AND RECORD KEEPING

When securing and handling evidence it should be assumed that all evidence may need to be presented in court and should therefore be treated accordingly.

All evidence should be kept securely, with access limited to those working on the investigation. Ideally investigatory meetings will be held off site.

Evidence such as computer data, transferable media, should only be handled by the companies approved IT Consultants, who themselves are fully signed up to Restore Compliances confidentiality terms and conditions. Where evidence, or other relevant information, is to be shared with another body, careful consideration should be given to the requirements of the Data Protection Act. Where there is any doubt, expert advice must be sought.

Clear records and logs of events, communications, key dates etc, must be kept, unnecessary records or copies and all papers relating to the investigation must be securely destroyed at the conclusion of the investigation and the communication of sensitive information via email should be avoided where possible

REPORTING OF FINDINGS

As with all investigations the results will be issued in a report format. The report will record, the scale of the incident/s, when and how it was perpetrated and by whom. In addition, the report will record; what action has been taken against the perpetrator, the actions to prevent further similar losses and to recover what has been lost. It will also note how the fraud was detected and whether or not existing controls were effective.

The report will be issued to the Executive only, who will review the findings. A copy will not be provided automatically to suspects or their representatives. However, if a disciplinary hearing takes place the individual and their representative will be entitled to receive a copy.

Any actions arising from the final report should be allocated to named individuals with appropriate due dates for completion.

COMMUNICATIONS

Communication should be clear and transparent at all time, to encourage reporting and instil confidence that concerns will be followed promptly and fairly. Assurances on confidentiality should also be given.

Third parties who may need to be alerted or informed may include the police, insurers and legal advisors. Established lines of communication should ideally already be in place with these groups to ensure that a timely and consistent approach is made and that the right information is passed on in the early stages of the investigation.

Care will be required on communicating with the person who raised concerns. It may be necessary to manage expectations as it may not be possible to maintain confidentiality, for example if disciplinary action is to be taken or a prosecution sought.

Jennifer Barrett – Director

Kathryn Morement – Director

April 2025

Review April 2028