Fraud, Bribery and Money Laundering Policy

Overview

Simplified Loader is committed to the highest ethical standards and is culturally aware of the prevention and detection of fraud, bribery, money laundering and financial crime including theft (hereon in collectively referred to as "Financial Crime") and will uphold all relevant UK legislation.

It requires its employees and any person working on behalf of the Company to act at all times with honesty, integrity, propriety, and due care in all matters, but particularly in the safeguarding of the Company, its associated assets, its reputation, and that of its organisational group.

The Company has a zero-tolerance approach to Financial Crime or any other form of corrupt behaviour and actively encourages anyone working with the business as an employee, contractor, client, or partner, to report breaches in procedures to the Company's Managing Director immediately. All reports will be dealt with in a safe and confidential manner (see 'Whistleblowing Policy') and will be investigated rigorously. Any breach of this Policy by a staff member may ultimately lead to dismissal via the Company's disciplinary procedure.

The purpose of this Policy is to set out individual responsibilities with regards to the prevention of, detection of and response to Financial Crime including what to do in the event of a suspected offence and what action will be taken by the Company in the event that an offence has been committed. The Policy is based on five key principles:

- **Principle 1:** It is based on risk and has been written to convey to employees the expectations of the Board regarding managing such risks.
- **Principle 2:** The risk exposure which is assessed by the Board to identify specific potential events that it needs to mitigate.
- **Principle 3:** Prevention techniques and controls to avoid potential risk events are established, where feasible, to mitigate potential impacts to the Company.
- **Principle 4:** Detection methods and controls are established to uncover risk events when preventative measures fail, or unmitigated risks are realised.
- **Principle 5:** A response process, including reporting, is in place to solicit inputs on potential risk events and a coordinated investigation approach is used to ensure potential offences are dealt with in a timely manner.

Who Is Affected By This Policy?

This Policy applies to the Company and all other parties who are given access to the Company's information and premises.

This Policy covers all persons whether:

- Employees of the Company
- Board/committee members of the Company
- Temporary agency staff or volunteers
- Consultants, contractors, and agents (whether employed on a casual or freelance basis or otherwise)

If the action taken by the Company includes disciplinary action in relation to a member of staff, the Company's disciplinary policy and procedure is followed.

Fraud

The Fraud Act 2006 broadly defines three main types of fraud:

- **Fraud by false representation** - where an individual dishonestly and knowingly makes a representation that is untrue or misleading.
- **Fraud by wrongfully failing to disclose information** - where an individual wrongfully and dishonestly fails to disclose information to another person when they have a legal duty to disclose it, or where the information is of a kind that they are trusted to disclose it, or they would be reasonably expected to disclose it.
- **Fraud by abuse of position** - where an individual who has been given a position in which they are expected to safeguard another person's financial interests dishonestly and secretly abuses that position of trust without the other person's knowledge.

The Act also includes offences of obtaining services dishonestly and of possessing, making, and supplying articles for use in frauds, and of fraudulent trading applicable to non-corporate traders.

For fraud to be committed under the legislation there will need to be an identifiable intent by the individual to make a gain or to cause a loss or to expose another to the risk of loss.

The Fraud Act 2006 does not apply in Scotland, where fraud is a common law crime and offences include "falsehood, fraud and wilful imposition". For the avoidance of doubt however, this Policy applies in full to Scotland.

Examples of fraud

Some examples of actions that could be considered to be fraud are as follows, although the list is by no means exhaustive:

- Theft of any company property
- Theft of petty cash / banking's
- Forgery or alteration of any document, for example a cheque
- Destruction or removal of records
- Falsifying expense claims
- Receiving incorrect salary overpayments and not informing or re-imbursing the Company
- Use of the Company's assets and facilities for personal use

- Fraudulent use of computer time and resources, including unauthorised personal browsing on the Internet

These last two examples would obviously exclude any reasonable, occasional but limited personal use, for example phone calls when away on company business or personal use of the computer in accordance with the Company's Acceptable Use Policy.

Bribery

Definitions/offences of bribery

- **Active Bribery** – offering, promising, or giving bribes
- **Passive Bribery** – requesting, agreeing to receive, or accepting bribes
- Failure of a commercial organisation to prevent bribery

Examples of Bribery

- Allocation of property without following approved allocations policies and procedures, in return for a reward
- Offering employment without following approved recruitment policies and procedures, in return for a reward
- Acceptance of gifts, goods and/or services as an inducement to giving work to any supplier
- Disclosing confidential information to outside parties without authority for personal gain

Unacceptable gifts include those that:

- Are illegal or involve a biased or dishonest act
- Would result in the violation of any law
- Involve conduct of a sexual nature and/or violation of mutual respect
- Create mutual agreements (requiring anything in return for the gift)
- Violate the Company Corporate Code of Conduct (See Gift Register guidelines)

Money Laundering

The Company mitigates money laundering risks effectively through:

- identifying our customers and knowing their ownership and control structure
- understanding our relationship with them

Internal controls and monitoring systems are in place to alert staff should criminals try to use the Company for money laundering, try to purchase goods fraudulently or to engage in any other Financial Crime.

Once aware of any potential threat, the Company will take steps to prevent it and report any suspicious activity to the National Crime Agency.

The Company is constantly vigilant to new types of Financial Crime and constantly looks to amend its control environment where necessary to respond to new threats.

Examples of money laundering activity

- Sudden changes in customer ordering, delivery and/or payment requests, or those who may agree to bear very high or uncommercial penalties or charges
- Other irregularities and/or suspicious transactions both within the Company and in organisations with which the Company contracts with

Authorized signatory

Puneet Vishnoi (General Manager)

Simplified Loader

Signed on: 05-Sep-2024