


Fraud Policy



Policy & Responsibilities

Document History

Date	Rev	Comments
01.02.22	01	Creation of Policy
09.04.24	02	Revision of Document

Prepared By		Date
Paul Clarke Managing Director		9 th April 2024

Policy Statement

Reachout Medical Ltd is committed to conducting its business with the highest standards of honesty and integrity. Fraud can take many forms. For the purpose of this policy fraud is defined as intentional deception of, or damage to an individual or an entity for financial or personal gain.

Reachout Medical Ltd takes a zero tolerance approach to fraudulent activity and all alleged or suspected fraud will be investigated thoroughly. Fraud is a criminal offence, and proven fraudulent activity will be treated as such.

Scope of the Policy

This policy covers all employees, contractors, agency workers, job applicants, consultants, suppliers and Clients/Participating Authorities.

Responsibilities

It is the direct responsibility of the Managing Director to ensure the implementation of this policy on a day-to-day basis, however, all employees, contractors, agency workers, job applicants, consultants, suppliers and Clients/Participating Authorities are also expected to act with honesty and integrity at all times.

Employees

Employees are required to accept their personal responsibility in applying our Fraud Policy. They must be familiar with its contents and ensure that it is followed by both themselves and employees for whom they have responsibility. Disciplinary action may be taken against any employee who acts in breach of this policy. Disciplinary action may include summary dismissal in the case of a serious breach or repeated breaches. In other cases, it may include a verbal or written warning, or other remedial action including training. Such action will be taken in accordance with the Company's disciplinary procedure. Breaches of this policy may also result in the employee responsible being held personally liable for compensation if legal action is taken in relation to fraudulent dealings.

Contractors and Agency workers

Contractors and agency workers are also expected to behave with integrity in all of their dealings, both with Reachout Medical Ltd and with its Clients/Participating Authorities.

Should a Contract or agency worker be proved to have behaved fraudulently or been involved in fraudulent activity, we reserve the right to terminate their assignment with immediate effect and take legal action accordingly.

Job Applicants

Job Applicants are also expected to behave with total integrity and provide information linked to their application that is accurate, honest and true. They are also required to confirm that they have not withheld any information of which the company should be made aware. Should the company become aware of dishonestly, deliberate inaccuracy (including provision of misleading information) or fraudulent activity during the application or registration process,

we reserve the right to terminate the application process with immediate effect and withdraw our services.

Consultants and Suppliers

As detailed previously, consultants and suppliers are also expected to behave with total integrity in all of their dealings with or on behalf of the company. If it becomes apparent that any such dealings could be construed as fraudulent or deliberately misleading, we reserve the right to terminate our dealings with the individual or entity with immediate effect.

Definitions of Fraud

Fraud is usually connected with monetary gain, however for the purpose of this policy; fraud will also be defined as intentional deception that is designed to:

- Mislead.
- Damage another individual or entity.
- Deprive another individual or entity.
- Achieve personal gain.
- Gain personal prestige.

For clarification, deliberate hoaxes that culminate in any of the above will also be treated as fraud.

Examples of Fraud

The following examples are provided purely for clarification and this is not an exhaustive list. They do not cover the full scope and range of potentially fraudulent activity, and should be treated purely as examples of the types of fraud that may be associated with a recruitment agency.

- Failure to account for monies received.
- Receipt of goods, services or other inducements for providing unfair advantage.
- Dealing inappropriately with company, contractor, agency worker or Client/Participating Authority transactions.
- Supply of free or reduced cost services to colleagues, friends or relatives.
- Misappropriation of contractor or temporary worker bank details.
- Falsification of expense claims.
- Authorising or receiving payment for hours not worked.
- Misuse of company assets or property.
- Breaches and misuse of intellectual assets.
- Falsification of records or unauthorised amendments to databases, administration systems or accounting records.
- Submission of fraudulent timesheets.
- Alteration, falsification or forgery of documents.
- Provision of deliberately misleading information.
- Deliberate withholding of essential/relevant information.
- Identity theft.
- Embezzlement of company funds.
- Cyber-crime, internet fraud or hacking.

Prevention of Fraud

Reachout Medical Ltd has a broad range of processes and procedures in place to prevent fraud. Employees are required to comply with these processes to minimise the risk of fraud. These include but are not limited to:

- Use of external accountants/auditors to review financial transactions and ensure probity of accounting practices.
- Examination of timesheets by experienced payroll staff to identify any potential fraud and validate any amendments.
- Requirement for any amendments to hours/timesheets to be authorised member of the Client's/Participating Authority's staff or submitted by secure online means.
- Electronic timesheets to be sent by email from an authorised member of the Client's/Participating Authority's staff or where online timesheets are in use, these must be approved by someone authorised to do so.
- Requirement for receipts to be provided for all expenses and for these receipts to be reconciled with a documented expenses claim.
- Compliance with the company's Ethics and Business Integrity and Anti-Bribery & Anti-Corruption Policies.
- Completion of the company's application form for applicants including signing the declaration confirming that the information provided is correct and that applicant has not withheld any information of which we should be made aware. The declaration also ensures that the applicant understands that giving any incorrect or misleading information could lead to their subsequent dismissal, withdrawal/termination of our services and where appropriate referral to the appropriate Counter Fraud Service or the NHS Counter Fraud Authority (by).
- Communication of and compliance with the following company policies:
 - Recruitment and Induction.
 - Training.
 - Verification of Identity and Address Procedure.
 - Verification of Right to Work in the UK Procedure.
 - Verification of Professional Registration Procedure.
 - Verification of Employment History and Referencing Procedure.
 - Criminal Records and Barring Check Procedure.
 - Work Health Assessment Procedure.
 - Data Protection.
 - Purchasing & Procurement.
 - Social Media.
 - Information Security.
 - Safeguarding.
 - Whistleblowing.
- Password protected company computer systems (including regular mandatory password changes).
- Paper files containing personal data and financial information to be retained in locked filing cabinets to prevent opportunist fraud.
- Policy of shredding of documents which contain personal data/information to prevent it being used for fraudulent purposes.

Reporting of Suspected or Alleged Fraud

Suspected or alleged incidences of fraud should be reported to the Managing Director immediately. Any employee, contractor, agency worker, consultant, supplier or Client/Participating Authority who has concerns that a fraudulent act may have taken place has a duty to report the matter to this member of our staff immediately. The company will take vigorous action against anyone trying to suppress a possible report of fraud.

Contact details for the Managing Director for reporting fraud are:

Name: Paul Clarke

Tel No: 07703 189354

Email: paul@reachoutmedical.co.uk

The Managing Director will assess the allegations/suspicious and decide upon the appropriate action to be taken. If the incident is considered to be very minor, then the situation may be dealt with directly and in the case of employees, the company's disciplinary and grievance procedure may be invoked as required. If the incident is of a more serious nature, the Managing Director will inform the appropriate Counter Fraud Service and the Police.

In all cases, the Managing Director is responsible for investigating any allegation of fraud and maintaining complete records of the suspicions raised or allegations made, including dates, times and persons involved, and actions taken.

Where it is suspected that such fraudulent activity may have been undertaken by a staff member and the alleged incident complies with the definition of a "qualifying disclosure", then reporting the matter will be done in accordance with the company's Whistleblowing Policy.

Review

This policy will be reviewed regularly and may be altered from time to time in light of legislative changes or other prevailing circumstances.