



GROUP FRAUD POLICY

1 Purpose

This policy details how each Cult Wines Group company (the Firm) will manage the risks posed by fraud and ensure a consistency of approach within the Group.

The Firm will act in accordance with the anti-fraud rules as defined by the relevant legislative and regulatory authorities.

The Firm has a zero tolerance for fraud and is committed to mitigating the risks of fraud. The Firm will take the necessary preventative actions and will promptly investigate any suspicion of fraud occurring.

2 Review of Policy

This policy will be reviewed regularly, at least once a year, and amended as considered necessary by the Firm's Management Body in the event of changing circumstances or regulations.

3 Responsibilities

3.1 Management Body Responsibilities

The Management Body of the Firm are responsible for assessing fraud risk, ensuring the implementation of this policy to minimise the risk and providing the appropriate employee training.

The Management Body will satisfy themselves that there are appropriate systems and controls in place for any outsourced arrangements to monitor and mitigate the risks posed by financial crime including fraud occurring at those providers.

The Firm has appointed Gemma Castle as the Nominated Officer with overall responsibility for the establishment and maintenance of effective financial crime (including fraud) systems and controls.

The Management Body will ensure that the Nominated Officer has a level of authority and independence within the Firm and that he/she has access to sufficient resources and information to carry out his/her responsibilities. The Nominated Officer will be subject to the Firm's performance management process to ensure ongoing competence in the role of Nominated Officer.

The Management Body will review the management information on financial crime including fraud provided to them to enable them to appropriately manage the financial crime risks and will take any necessary actions.

The Management Body commits to provide the necessary authorities with the required access or information in the case of a financial crime investigation.

3.2 Nominated Officer

The Nominated Officer has responsibility for oversight of the Firm's compliance with the rules and regulations against fraud. The Nominated Officer will act as a focal point within the Firm for all activity relating to fraud prevention and detection. The Nominated Officer will be based in the UK. His/her responsibilities include:

- promoting an anti-fraud culture;
- appropriate risk management;
- fraud prevention and detection measures and;
- fraud investigation.

The Nominated Officer is responsible for keeping up to date with changes in laws and regulations in relation to financial crime including fraud and making use of findings from national and international bodies tasked with combatting financial crime in order to update the Firm's systems and controls where necessary.

The Nominated Officer is responsible for oversight of the Firm's compliance with its requirements in respect of staff training with regard to financial crime and fraud.

The Nominated Officer is the point of contact for all employees to raise any reports or concerns relating to any suspected or actual financial crime and is responsible for recording, investigating and reporting this to the relevant authorities, such as the National Crime Agency (NCA) in the UK, as necessary. Where reporting to the authorities is not deemed necessary the Nominated Officer will document the reason for this course of action.

The Nominated Officer is responsible for liaison with the law enforcement authorities as required.

The Nominated Officer will provide management information to the Management Body regarding the compliance with the policy, operation and effectiveness of the systems and controls in place to combat fraud, and recommendations or enhancements required, on at least an annual basis. The Nominated Officer will also escalate financial crime issues to the Management Body as considered necessary.

3.3 Senior Managers

All Senior Managers within the Firm are responsible for:

- ensuring that an adequate system of internal control exists within their area of responsibility and that controls operate effectively;
- preventing and detecting fraud;
- assessing the types of risk involved in the operations for which they are responsible;
- reviewing and testing regularly the control systems they are responsible for;
- ensuring the controls are complied with and their systems continue to operate effectively;
- implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place;
- incorporating anti-fraud controls at the design phase in all systems.

3.4 Employee Responsibilities

This policy will be communicated to all staff during their induction to the Firm and any updates will be communicated by the Nominated Officer.

All employees are expected to attend and complete the appropriate financial crime and fraud training. They will confirm that they have read and understood this policy on an annual basis.

All staff must show due regularity and propriety in the use of Firm resources and the handling of client assets, whether they are involved in cash or payment systems, receipts or dealing with suppliers. They must be alert to the possibility of fraud and take special care where individuals could be more vulnerable to committing fraud and where unusual transactions may occur. Employees are expected to be alert to money laundering, fraud, bribery, corruption, financial sanctions and all other forms of financial crime and they are responsible for reporting any actual or suspected financial crime to the Nominated Officer in a timely manner.

If suspicious signals of financial crime including fraud are identified these should be reported to the Nominated Officer. All suspicious signals of financial crime including fraud are reportable, even if it comes to the employee's attention after the transaction has been undertaken or the account is closed, or the transaction has been conducted by another person.

Employees must report details immediately through the appropriate channel if they suspect fraud has been committed or see any suspicious acts or events. They must co-operate fully with any internal checks, reviews or investigations into fraud.

Failure to notify an appropriate person about any criminal actions of which an employee is or should have been aware, in breach of this policy, may lead to disciplinary action and personal criminal liability.

3.5 Audit Function Responsibilities

The Firm has an external audit provider which is independent from the compliance and business functions. The audit team will review the adequacy and effectiveness of the Financial Crime framework including fraud prevention and detection policies, procedures, systems and controls. Furthermore, the audit team will measure compliance with the Financial Crime framework and make recommendations for improvements.

4 Definitions

For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party. The UK Fraud Act 2006 defines three categories of fraud:

- by false representation
- by failure to disclose information
- by abuse of position.

Fraud is used to describe such acts as theft, deception, bribery, corruption, forgery, extortion, embezzlement, misappropriation, false representation, concealment of material facts, collusion, false accounting and conspiracy to commit these offences. Fraud is committed by the act of seeking improper benefit. A crime is committed with the actual intention to defraud irrespective of whether it is successfully carried out. Examples include:

- forgery or alteration of payable order, expense claims, cheques, drafts, letters of comfort, contracts etc;
- any misappropriation of funds, supplies or any other asset owned or managed or service provided by the Firm;
- any irregularity in the handling or reporting of any transactions;
- misappropriation of and misuse of Firm or client property, equipment, materials, information or records;
- seeking or accepting anything of material value from vendors, consultants or contractors doing business with the Firm;
- any computer related activity involving the alteration, destruction, forgery or manipulation of data for fraudulent purposes or misappropriation of Firm owned software;
- any claim for reimbursement of expenses not incurred completely and exclusively in the performance of one's official duty;
- any similar or related irregularity.

4.1 Consequences of non-compliance

The Group will not accept any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately.

Non-compliance with the fraud prevention and detection obligations by employees is considered a serious offence and disciplinary actions may be taken by the Firm, including immediate dismissal.

Failure to comply with the law may also result in a criminal penalty (including imprisonment). The Bribery Act 2010 introduces a new offence which could lead to the Firm facing criminal liability and therefore the requirements of the new Act need to be considered in the event that any staff either bribe colleagues to commit a fraud or are themselves bribed to commit a fraud, as the Firm could itself become criminally liable under the Act. The offence of bribery not only covers staff, but also consultants or intermediaries acting on behalf of the Firm.

Penalties will vary by jurisdiction. In addition to these criminal penalties, a breach of these rules could cause significant damage to the reputation of the Firm and its employees. Failure to comply by an employee may expose the Firm to penalties, censure and enforcement action by authorities.

5 Risk management and Controls

5.1 Prevention

Line managers must ensure the security of assets and funds within their area of responsibility. Among the measures they can use to discharge this responsibility are:

- regularly assessing the exposure to potential fraud or theft;
- ensuring there is an adequate procedure for reporting problems to senior management;
- being aware of the Group's policy and procedures on fraud;
- assessing the suitability of staff to handle particular risk areas;
- ensuring appropriate segregation and rotation of duties;
- providing adequate training and guidance;
- ensuring regular management review of work; and
- ensuring complete and clear documentation of all transactions.

In addition to mitigating against fraud within the organisation, staff must also be aware of online fraudulent/phishing activities and must be extremely cautious when sharing information online about the Firm or its clients.

5.2 Fraud response and investigation plan

The Firm's Fraud Response and Investigation Plan sets out how to report suspicions and how investigations will be conducted and concluded.

5.2.1 Objectives

The objectives of the Fraud Response and Investigation Plan are to ensure timely and effective action is taken in order to:

- prevent losses of funds or other assets where fraud has occurred and to maximise the recovery of losses;
- minimise fraud by taking rapid action at the first signs of a problem;
- identify the fraudsters and maximise the success of any disciplinary and legal action taken;
- identify any lessons to help manage fraud in the future; and
- reduce adverse effects on the Firm and clients.

5.2.2 Staff Responsibilities

5.2.2.1 Reporting a suspected fraud

The route staff will take will depend on whether they are reporting a possible fraud undertaken by a member of staff or a member of the public. When they suspect a fraud they should not discuss this with any other work colleagues, either before or after reporting it to the appropriate person.

5.2.2.2 Fraud by a client or member of the public

If the fraud happens in a staff member's area they must report this to their line manager immediately. The line manager will then contact the Nominated Officer, who will then advise Senior Management as appropriate.

5.2.2.3 Fraud by a member of staff including consultants

If a work colleague is committing the fraud, then once again under normal circumstances staff should report this to their line manager. The latter will then contact the Nominated Officer, who will then inform Senior Management as appropriate. If staff suspect their own or any other line manager of committing a fraud, they should report it to someone else within the management hierarchy or use the Whistleblowing procedure.

5.2.2.4 What happens when staff report a fraud

When a fraud is reported, whether internal or external, an appropriate officer investigates it. Irrespective of the source of the suspicion, management must undertake an initial investigation to ascertain the facts.

Any conversations and information that staff disclose to the investigating officers will as far as possible remain confidential. They may be asked to produce a written statement that could be used in the event that the fraud becomes a criminal investigation. If staff are required to produce a written statement, they will receive help and guidance.

5.2.3 Management responsibilities

Every line manager is responsible for ensuring that procedures and systems exist within their area of responsibility to minimise the incidence of, and the risk of, fraud and irregularities.

Whenever any suspected fraud in the Firm is reported, the Nominated Officer shall be responsible for managing the investigation.

It is important that line management responsibilities with respect to the investigation are limited to assessing the evidence and determining whether the suspicion is reasonable, i.e. not malicious or based on a clear misunderstanding or lack of knowledge. Management must err on the side of caution. The advice of the Nominated Officer must be sought in all but the most straightforward of cases. Assistance by the Nominated Officer will be provided to manage or undertake the investigation as appropriate.

5.2.4 Evaluation and investigation of complaints and allegations

The facts and circumstances of frauds will vary, but it is important that all cases are rigorously and promptly investigated and that appropriate action is taken. As soon as an allegation is received, it is the responsibility of the line manager to undertake an initial enquiry to ascertain the facts. This enquiry should be carried out as soon as possible with the objective of either substantiating or repudiating the allegation that has been made. At this point care has to be taken to ensure that any activity is carried out in accordance with the UK Regulation of Investigatory Powers Act 2000 or local equivalent.

If the line manager has grounds for suspecting that a member of staff may be involved in a fraudulent activity, they should not interview the member of staff without seeking guidance from the Nominated Officer.

The purpose of the initial enquiry is to ascertain whether there is any substance in the suspicions so that, if necessary, a full investigation can be instigated. If the allegation is substantiated, the Nominated Officer should be briefed on the situation and will in turn inform Senior Management. At this stage, line managers should also bear in mind that they have a prime role in securing evidence and minimising any further losses. The Nominated Officer will offer advice on the most appropriate course of action. This further action may include the commissioning of specialist services to assist with the investigation e.g. forensic auditors, legal or IT specialists.

5.2.5 Allegation against an employee

If an allegation is substantiated after the preliminary enquiry and further investigation is required, the next steps in the investigation will be determined by:

- whether the employee should be subject to the Firm's disciplinary policy;
- whether there is evidence that an employee has committed fraud against the Firm or a client or has committed a corrupt act, in which case the employee may also be subject of a criminal investigation by the police.

5.2.6 Allegation against a client or member of the public

If an allegation is substantiated after the preliminary enquiry and further investigation is required, the type of investigation will very much depend on the allegation.

Generally all investigations will follow a criminal route; this will be with a view to prosecuting the individual under the appropriate legislation. The decision to prosecute will be finalised after the Firm has sought appropriate legal advice.

5.2.7 Management's welfare responsibility regarding an employee accused of fraud

The Firm may suspend and member of staff involved in a potential fraud, pending the outcome of the investigation. The HR team will be involved in this process.

Managers should be mindful of the Disciplinary policy. The Firm recognises that suspension can be an extremely stressful experience for employees as well as their families and managers should remind employees of the various support options which are available to them.

5.2.8 Subsequent investigations

The Firm is committed to supporting regulators and law enforcement authorities in the prevention of financial crime.

All employees are expected to cooperate fully with any investigation. Employees must also recognise, however, that laws and procedures may apply to the disclosure of information and they should therefore contact the Nominated Officer before disclosing information about clients or employees if they are contacted directly by law enforcement authorities.

5.2.9 The control framework to minimise and prevent fraud

When fraud has been identified, Senior Management should review the control procedures to ensure the risk of the fraud recurring are minimised.

5.2.10 Press and Publicity

External communications will be dealt with centrally by Senior Management in all matters regarding fraud and corruption. If staff disclose any related information to the media without the express authority of the CEO, this will be regarded as a disciplinary offence.

5.3 Training

The Firm should ensure that all staff and managers receive training in fraud awareness. The level and the extent will depend on the work that the individual carries out. When employees are an integral part of the control framework their knowledge must be refreshed on a regular basis.

5.4 Monitoring and detection

The Firm will continually monitor its own activities as well as its clients’.

5.4.1 Red Flags

A number of frauds can come to light because of suspicions aroused by, for instance, the behaviour of certain individuals or cases where individuals are more vulnerable due to a change in circumstances. Red flags are behaviours or issues which should act as a warning that further investigation by the Firm might be necessary. The following are warning signs that might indicate that fraud may potentially be taking place:

- Unusual behaviour, reluctance to take leave, refusal of promotion or regular long hours worked by key staff. When an employee is on leave the work is left until the employee returns.
- Key documents missing, documents that are lacking key information. Missing expenditure vouchers and official records.
- A sudden unexplained change of lifestyle or an employee's lifestyle that is more affluent than would be expected from his/her employment.
- A change in an employee's circumstances that could have left them more vulnerable to committing fraud.
- Cosy relationships with suppliers/contractors. Suppliers/contractors that insist on dealing with one particular member of staff. Excessive variations to budgets or contracts. Defining needs that can only be met by specific contractors. Lowest tenders or quotes passed over with minimal explanation recorded. Single vendor selection and vague specifications. Disqualification of any qualified bidder.
- Managers bypassing subordinates, subordinates bypassing managers and managers frequently overriding internal controls.
- Lack of Senior Management oversight. Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluating).

Also refer to the Anti-Money Laundering Policy for examples of client-related red flags.

5.5 Reporting Fraud and Suspicious Transactions

Employees are expected to be alert to fraud and they are responsible for reporting any actual or suspected fraud to the Nominated Officer via their line manager in a timely manner.

Where there is serious suspicion, evidence or reasonable grounds for suspecting that a client transaction may be deemed suspicious, employees are required to report their suspicions in accordance with the Firm's procedures for Suspicious Activity Reporting.

The Nominated Officer will receive any reports or concerns relating to any suspected or actual fraud and will record, investigate and report this to the relevant authorities, such as the National Crime Agency (NCA) in the UK, where necessary. If reports are not forwarded to the relevant authorities, full details of the rationale for this decision will be kept on record.

All notifications made will be handled with strict confidentiality. However, there may be circumstances whereby the Firm is required to reveal an individual’s identity, for example where the Firm is compelled to do so by law and therefore anonymity cannot be guaranteed.

If there are concerns about any repercussions of reporting a suspicious transaction or fraud, then the Whistleblowing Policy and Procedure should be followed for information on alternative methods of making a report.

Failure to notify an appropriate person about any criminal actions of which an employee is or should have been aware, in breach of this policy, may lead to disciplinary action and personal criminal liability.

5.6 Record Keeping

The Firm will keep the following records for a period of at least 5 years:

- Transaction records (carried out with or for a client)
- Records of any internal reports made to the Nominated Officer and of any external reports made by the Nominated Officer
- Where the Nominated Officer has considered information or other matter concerning knowledge or suspicion that another person has engaged in fraud, but has not made a report to the National Crime Agency, a record of that information or other matter

The Firm will keep records of fraud and criminal investigations for at least 10 years after the action or investigation is completed.

These records are kept at the Firm’s offices and the Nominated Officer is responsible for ensuring that these records are complete and up to date.

6 Breaches of Fraud Policy

Any breaches of the Fraud Policy will be recorded on the Firm’s breach register. Failure by employees to comply with this policy may lead to disciplinary action and personal criminal liability.

Owner	Gemma Castle
Version	V1.0
Approved on	21 st February 2022
Target Audience	All personnel, contractors and consultants.