CLARKSONS

COMPLIANCE MANUAL 2023

Statement from the Board of Clarkson PLC

ETHICAL BEHAVIOUR

The Clarkson group of companies ("the Group") is the world's leading provider of integrated shipping services with an exceptional breadth of expertise, especially in ship broking, finance, research, port services and other aspects of shipping. It is founded on a commitment to provide the highest quality of service to our clients while maintaining the highest level of integrity. It is premised on acting pursuant to this code and all applicable laws and regulations of the countries in which we operate. Upholding these commitments is essential to our success.

PURPOSE OF THIS CODE

This Compliance Code/Manual ("Code"/"Manual") sets out both the Group's standards of conduct and certain of its legal obligations. Given that the Group has operations in many countries, employees, directors, non-executive directors and officers (collectively "Employees") doing business internationally must, in addition to the Code, comply with applicable laws and regulations in the countries concerned (the "Laws").

This Code and the Laws apply to all the companies in the Group and all Employees. The Group may also work with third party agents and consultants. Before doing so, we will seek their cooperation in adhering to this Code.

Employees without any exception must comply with the Laws and the Code. If you are unsure what is required of you, you must ask either your office Managing Director ("MD"), General Counsel/Head of Legal ("Legal") or the Group Company Secretary in accordance with the procedures in this document.

Failure to comply with this Code may result in disciplinary action against an Employee, including but not limited to a warning, suspension or termination of employment. In addition to consequences imposed by the Group, violations may result in referral to civil or criminal authorities where appropriate.

Each member of the Board has studied this Code carefully and has signed a statement confirming that they have done so. We expect all Employees to digitally read the Code via our learning management tool and to digitally confirm that they have read it, understood it and will comply with it.

COMPLIANCE PROCEDURE

Employees must:

- Review the Code and ensure that they adhere to this and their contract of employment at all times.
- Report without fear all types of violations or potential violations of this Code in accordance with the terms of this Code as set out on page 22.
- If in doubt, consult their MD, Legal or the Group Company Secretary.

The Group will implement the Code through on-going training, monitoring and review. The Code is also available on the intranet (hosted on the Group Directory) and may be amended from time to time.

Ultimately, our most valuable asset is our reputation. Complying with the principles and standards contained in this Code is the starting point for protecting and enhancing that reputation. However, not every situation can be covered in this Code. You are entrusted to use good judgment and common sense in your daily activities. Ultimately, your personal integrity and honesty defines the character and legacy of our Group.

Thank you for your commitment.

On behalf of the Board of Directors of Clarkson PLC

Contents

Introduction

EMPLOYEE RESPONSIBILITIES

As a matter of Group policy, compliance with this Code is a requirement of continued employment with the Group. Failure to comply with any policies and procedures in this Code may result in disciplinary action against the Employee, including but not limited to a warning, suspension or termination of employment. In addition to consequences imposed by the Group, violations may result in referral to civil or criminal authorities where appropriate.

This Code is the property of the Group and its contents are strictly confidential.

HOW TO USE THIS CODE

This Code is presented in sections which sets out some core compliance requirements under which the Group operates. Generally, for each compliance topic a summary of relevant law is provided (Law), followed by a statement of the Group's policy on the issue (Policy) followed by the procedures through which the policy will be implemented (Procedure). The goal of the Procedure is to specify what each Employee must reasonably do to comply with the Code or Laws and what Employees should do if there is an actual or suspected breach.

REPORTING VIOLATIONS

Unless a particular policy of the Group specifically provides that violations are to be reported directly to Legal or the Group Company Secretary or Money Laundering Reporting Officer ("MLRO"), Employees must report any violation promptly to Legal or anonymously in accordance with the Whistleblowing Policy. Any such reports will be treated confidentially to the extent permitted by law. Legal, Group Company Secretary or MLRO will endeavour to resolve any such violation or suspected violation of the provisions of this Code within 90 days of the report thereof, including investigating the reported or suspected violation, issuing a report to management on the factual findings and recommending sanctions, where appropriate. Employees are required to cooperate in any investigation.

Retaliation against an individual who reports a violation is prohibited and will be dealt with as a separate breach of Group Whistleblowing Policy.

If in doubt, ASK.

CONTACTS

GROUP COMPANY SECRETARY

Deborah Abrehart
E. Deborah.Abrehart@Clarksons.com
T. Ext 3185

MLRO

Mike Cahill
E. Mike.Cahill@Clarksons.com
T. Ext 3168

GROUP GENERAL COUNSEL/ HEAD OF COMPLIANCE

Sandra Rosignoli
E. sjr@Clarksons.com
T. Ext 3165

COO

Jeff Woyda
E. Jeff.Woyda@Clarksons.com
T. Ext 3004

Conflicts of Interest

THE LAW

Conflicts of interest arise when two or more interests compete and such conflicts potentially compromise judgment and independence. For example, it is a conflict of interest if Employees compete with the Group, by working, advising or engaging in business for a competitor, customer or supplier of the Group. Judgment may become impaired and Employees may face situations which may prevent them from acting objectively or effectively. Whilst the existence of conflicts does not imply that improper acts have taken place, they do significantly increase the necessity for extra care to ensure that such acts are avoided.

POLICY

The Group has specific policies around certain potential conflict of interest situations as follows:

External directorships and interests

It is the Group's policy that its employees devote their full working time and attention to the business of the Group. Business activities including appointment to any office or employment (paid or unpaid) of any nature other than for the Group are not permitted without written permission. You must obtain written permission from either your MD or HR before you accept any offer of secondary employment, or engage in any consultancy or advisory work or actively engage in other business activities. Permission may be granted if your proposed role is unlikely to present any real or potential conflict of any kind with the interests of the Group or interfere with your duties generally but the Group reserves the right to refuse permission or revoke permission previously granted in its sole discretion.

Each year any of you who are directors will be required to sign a declaration of directors' interests which will be retained by the Group Company Secretary. The creation and operation of a personal website is subject to this general policy if the site has any business or commercial application. There must be no direct reference to or implied association with the Group or any of its clients or suppliers and you must not use the Group logo on the site without permission from HR. Additionally, any use of hyperlinks to the Group is prohibited without permission from HR. There must not be any recognisable references to the Group, whether implicit or explicit, in any online diary entries or postings or online video sites including for example, but not limited to, YouTube, Twitter, Facebook, Tumblr or Instagram without permission from HR.

Private and personal share dealing

As a result of your duties, you may have access to inside information as defined in relevant legislation and/or be in a position where your share dealing transactions might be, or might give the appearance of being, in conflict with the interests of the Group or any of its shareholders, customers or clients. Dealing for yourself or for persons connected with you in these circumstances or encouraging others to deal is not acceptable and may be a criminal offence or be in contravention of the regulations to which the Group and its Employees are subject. To this effect, please refer to the Insider Dealing section in this Manual.

In order to protect you and the Group from contraventions of governing laws, regulations or generally accepted industry standards, all share dealing for you and your connected persons (this includes persons connected to you by blood, business or relationships) must be conducted in accordance with the detailed instructions given in the Insider Dealing section. Before dealing for yourself or your connected persons, you must make yourself familiar with the terms of this policy and the Company's Share Dealing Rules.

Procedure

Employees must ensure that they have read and comply with the Insider Dealing section of the Code and the relevant share dealing policies referred to therein and Employees must read and comply with the relevant provisions in their employment or consultancy contracts relating to conflicts of interest.

Employees must disclose to the Group Company Secretary any share dealing that could give rise to any conflicts, either personally or for others, whether actual or potential.

Employees must disclose to their MD any transactions or relationships that could give rise to any conflicts, either personally or for others, whether actual or potential.

All further actions in relation to such transactions or relationships are strictly prohibited unless and until they are approved by their MD in writing or, if in respect of share dealing, by the Group Company Secretary.

Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

Insider Dealing

The Board of Clarkson PLC has recently revised its share dealing rules and these rules may be found on the intranet. These rules cover both criminal and civil restrictions imposed by law regarding the dealing in securities when Employees and members of their household may be or are in possession of inside information.

THE LAW

What is insider dealing?

Insider dealing is the illegal trading in shares or financial instruments by someone or at the instigation of someone on the basis of information that is not yet publicly known and which information would likely affect the price of shares or financial instruments if it were made public.

Many jurisdictions have "insider dealing" laws including the UK and the US. There are some differences between different jurisdictions however the broad principles set out below remain relevant to all.

Who is an insider?

An insider can include, amongst Employees and members of their household and the Group's external lawyers, advisers, accountants, consultants and bankers. An Employee of the Group could become a temporary insider to another company because of the Group's and/or employee's relationship to such company (e.g. by having contact with company executives while researching the company).

What is inside information?

Inside information is information of a precise nature, which has not been made public, which relates directly or indirectly to a company and its subsidiaries or its shares or related financial instruments and which, if it were made public would likely affect the price or value of these shares or related financial instruments.

Information is likely to have an effect on price if it is information that a reasonable investor would be likely to use as part of the basis of his or her investment decisions.

Information that Employees should consider price-sensitive includes but is not limited to non-public information about financial results or forecasts, significant new contracts or other arrangements, gain or loss of a substantial client, possible mergers or acquisitions, joint ventures, investments, divestments and/or changes in senior management.

If you are in any doubt about whether information you become aware of is "inside information" you should ask the person providing you with the information AND refer it to the Group Company Secretary.

What is non-public information?

Information is non-public until it has been effectively communicated to the marketplace. You must be able to point to some fact to show that the information is generally public. For example, information appearing in the Financial Times, Reuters Economic Services, the Wall Street Journal or other publications of general circulation would be considered public. Similarly, information released over computer based news services in communications to shareholders or widely distributed by prospectuses followed by a passage of time sufficient for the investing public to absorb the information constitutes effective communication to the marketplace. Information that is available only to a select group of analysts, brokers or institutional investors is not public information. Undisclosed facts that are the subject of rumours, even if widely circulated and even if they turn out to be accurate, do not constitute public information that allows you to claim non-public inside information has become public.

What is tipping?

Tipping involves providing price-sensitive non-public information to anyone who might be expected to trade while in possession of that information. An Employee may be a "tipper" by passing on price-sensitive non-public information in breach of this Code. An Employee may become a "tippee" by acquiring price-sensitive non-public information from a tipper, which would then require the Employee to follow the procedures below for reporting and limiting use of the information.

Penalties for insider dealing

Penalties for dealing on or communicating price-sensitive non-public information are severe, both for individuals involved in such unlawful conduct and their employers, and may include imprisonment, fines or damages. A person can be subject to some or all of the applicable penalties even if he or she does not personally benefit from the violation. In addition, insider dealing could result in serious sanctions by the Group, including dismissal.

POLICY

Dealing

The Group forbids all Employees to trade or invest in shares, either personally or on behalf of others, while in possession of price-sensitive non-public information with respect to such shares or to communicate price-sensitive non-public information to others other than to those who have a need to know in connection with the performance of services to clients and to the Group.

Dealing means more than just buying and selling of securities. It can include entering into options, assignments, using securities as security or a promise to buy or sell such securities.

The Group forbids all Employees to deal in Clarkson PLC shares during a "close period" in accordance with the Employee Share Dealing Code.

The Group forbids any Employee with inside information to deal in Clarkson PLC shares without obtaining clearance to deal in advance in accordance with the Employee Share Dealing Codes provided to you and available on the Group intranet. Before dealing in shares persons discharging managerial responsibility ("PDMR's") and the Group Company Secretary must always obtain consent from the chairman of Clarkson PLC, the chairman must always obtain consent to deal from the CEO or the senior independent director if the CEO is not available. You will be informed if you are a PDMR by the Group Company Secretary.

The Group forbids dealing in derivatives linked to any Clarkson PLC shares or engaging in short selling of any such shares at any time under any circumstances. Clearance will not be granted in relation to such dealing.

Employees are required, where possible, to use the Company's share dealing service provided by its designated Stockbrokers. There will be circumstances where this is mandatory in order to maintain an orderly market. Please contact the Group Company Secretary if you need any information about the share dealing service.

Additional restrictions apply to Employees who have been designated as "insiders" under the Market Abuse regime and they must abide by the additional provisions of the Group's Securities Dealing Code.

Security

Employees must not discuss price-sensitive, non-public information with anyone, to others other than to those who have a need to know in connection with the performance of services to clients and to the Group.

Enquiries from third parties, such as industry analysts or members of the media, about the Group or any of its clients must be directed to your MD, Legal or the COO.

Employees must take precautions to safeguard price-sensitive, non-public information. Accordingly, employees should conduct business and other activities so as not to risk inadvertent disclosure of price-sensitive, non-public information. Employees must take extreme caution not to disclose any price-sensitive, non-public information through the use of social media or social networking websites nor mention any Group-related matters.

Confidentiality

All information about clients and the Group's activities are to be kept in strict confidence by those who receive it, and such information may be divulged only within the Group and to those who have a need for it in connection with the performance of services to clients and the Group.

Even after an Employee is no longer employed by or affiliated with the Group, he or she must maintain the confidentiality of any price-sensitive non-public information obtained during such employment or affiliation.

PROCEDURES

The following steps should be taken by any Employee who comes into possession of information that is price- sensitive and non-public and that relates to (a) publicly listed shares or financial instruments not related to the Group; or (b) matters concerning the Group:

1. Do not deal on behalf of yourself or others with respect to the shares or financial instruments in question.
2. Do not communicate price-sensitive non-public information inside or outside the Group.

Documents and files that contain price-sensitive non-public information must be handled securely in order to minimize the possibility that such information will be transmitted to an unauthorized person. Such documents and files must be stored in locked filing cabinets or other secure locations and confidential information accessible by computer should be maintained in computer files that are password protected or otherwise secure against access by unauthorized persons.

As Employees are not permitted to discuss price-sensitive non-public information with, or in the presence of, persons who are not authorized to receive such information, they should thus avoid discussions of price-sensitive non-public information in hallways, lifts, and other open areas (including within the Group's buildings), trains, airplanes, restaurants and other public places generally. The use of speaker phones or mobile telephones also should be avoided in circumstances where such information may be overheard by unauthorized persons.

Employees are obliged to disclose to the Group Company Secretary, any potential insider dealing issues.

If you have any questions or are in any doubt as to how to comply with these rules, please contact the Group Company Secretary for further information.

Any Employee who fails to comply with the Employee Share Dealing Code, the Group's Securities Dealing Code and this Code will face internal disciplinary procedures which could result in dismissal for misconduct or gross misconduct and could lead to civil or criminal investigation or penalties.

Anti-Money Laundering

THE LAW

What is Money Laundering?

Money laundering means exchanging money or assets that were obtained criminally for money or other assets that are 'clean'. The clean money or assets do not have an obvious link with any criminal activity. Money laundering also includes money that is used to fund terrorism, howsoever it is obtained.

Money laundering is not something that occurs only in connection with obvious crimes such as drug traffickers. Receiving money or assets resulting from illegal acts such as criminal fraud, bribery or corruption (whether in the UK or overseas) and tax evasion can amount to money laundering. For example, the money saved from evading tax or customs duties is proceeds of crime and is thus capable of being laundered. Bribes purporting to be commissions that transfer through the Group to a fraudulent or corrupt co-broker or someone not entitled to them are the proceeds of crime.

In your work you may unwittingly be part of the technique being employed by a money launderer. The money launderer wants you and your company to be part of the unwitting series of people doing their legitimate job of handling and processing money. The 'dirty' money comes to your company as part of its legitimate business and in doing your job you and your company 'cleans' it and pass it on. You become part of the 'placement' and 'layering' techniques employed in money laundering (see next paragraph). That is why the suspicious activity reporting requirements at the heart of anti-money laundering laws are focused on honest people like you who because of the job you do are being exploited by a money launderer.

Money laundering is a major crime carrying harsh penalties. The maximum penalty on conviction of any of offences of arranging, concealing and acquisition (described below) is, for example in the UK, fourteen years imprisonment and five years for a tipping-off offence (described below).

Money Laundering Offences

There are various money laundering crimes (which vary depending on whether the Group entity involved is a regulated or unregulated entity) that you might commit as you are doing your job. These may include:

1. Arrangement – If you are a part of an arrangement to help conceal, disguise, convert or transfer money or other property that you know or suspect is the proceeds of a crime.
2. Concealing – You would be committing a money laundering act if you in any way concealed money or property that you knew or suspected was the product of a crime.
3. Acquisition, use and possession - If you acquire, use or possess money or other property that you know or suspect is the proceeds of a crime.
4. Failing to report - If you fail to report knowledge, suspicion, or where there are reasonable grounds for knowing or suspecting that another person is engaged in money laundering.
5. Tipping-Off/Prejudicing an Investigation – If after you have made your suspicious activity report (see paragraph 'Reporting') you do anything or say anything that may prejudice an investigation, you may commit the crime of Tipping-Off if regulated or Prejudicing an Investigation if unregulated. To avoid this follow the golden rule: report to the Money Laundering Reporting Officer (MLRO) and keep quiet.
6. It is also a separate offence for regulated businesses not to establish adequate and appropriate policies and procedures to prevent money laundering.

An offence can happen because in the course of your work you know something or suspect that money you and your company are handling is proceeds of crime but nevertheless you continue with the transaction instead of stopping and reporting your knowledge or suspicion to the MLRO. Failure to stop and report may make you a money launderer.

Recognising Money Laundering

It is not easy to point to a clear cut instance of money laundering that you may come across in your work. Indeed in our business, given that we primarily deal with clients well known to us and to the market, we will not be an obvious target for money launderers but here are some examples of the kinds of things that could be indications of money laundering:

Employees and Agents

- Changes in behaviour (e.g. lavish lifestyles or avoiding taking holidays).
- Changes in performance (e.g. broker has a remarkable or unexpected increase in performance).
- Any dealing with someone where the identity of the ultimate beneficiary or true counterparty is undisclosed contrary to normal procedure for the type of business concerned.

Abnormal transactions

- Transactions not in keeping with the client's normal activity, normal market behaviour or the business that the client operates i.e. an address commission that is so large it may distort the underlying nature of the transaction in order to mislead.
- Transactions where any payments including commissions are credited to a different account from that set out in the original contract or to third parties including consultant or nominees not involved in the transaction.
- Transactions where any payment is made to a fraudulent or corrupt co-broker.
- Transactions where any payments including commissions are credited to unverified third parties.
- Split invoices to different parties one or more of which is not linked to the transaction and has not been verified.
- Requests to issue an invoice for less than the contractual amount.

None of the above NECESSARILY involves money laundering, and there may be other kinds of transactions and behaviour which are suspicious that are not on the list. However the following should always be considered before entering into a transaction: -

- Is the client/broker/recipient known to you?
- Is the transaction in keeping with the normal business activity of that party?
- Why are the payment arrangements not straightforward? e.g. is payment to be made to an apparently unconnected third party and if so has the third party been verified?

POLICY

The Group endeavours to prevent its Employees and companies from being used for money laundering and terrorist financing.

The Group has separate and specific policies for its regulated businesses to actively combat money laundering and terrorist financing.

PROCEDURES

The Group has put in place procedures to combat money laundering. These include:

1. The guidance provided in this Code and the anti-money laundering policies in place for regulated businesses in the Group ("Regulated AML Codes").
2. Know Your Client ("KYC") due diligence procedures for regulated and non-regulated businesses.
3. An AML and KYC Manual for unregulated businesses.
4. Presentations and training courses from time to time for MDs and accounts/finance and Employees of regulated and unregulated businesses in the Group.

All Employees must be aware of their legal and regulatory requirements by reading this Code and all Employees working for regulated businesses must be aware of the increased legal and regulatory requirements by reading the Regulated AML Codes.

All Employees must attend the relevant AML courses, where applicable.

If you have knowledge or are suspicious about a particular transaction, or have reasonable grounds for knowing or suspecting, that someone else is or has been involved in money laundering activity, you must REPORT the details to Legal or the MLRO as soon as practicable.

To protect yourself and the Group from potential prosecution, you should act as follows:

1. During the course of any transaction, you should be alert to the possibility of money laundering activity and satisfy yourself that the transaction in question is legitimate and does not involve criminal property;
2. If, during the course of any transaction, you become aware or suspect that criminal property is involved, you should immediately report the circumstances to Legal or the MLRO who will advise you of next steps;
3. Having reported the circumstances, you must not take any further steps in the transaction unless authorised in writing by the MLRO or Legal, as the case may be;
4. Once you report the circumstances, you must not inform the client or anyone else that you have done so. If you do you may be guilty of a "tipping off" or "prejudicing an investigation" offence;
5. If, after reporting the circumstances, the MLRO or Legal authorises you in writing to carry on with the transaction, then it will be safe for you to do so and (provided you have complied with the above paragraphs) you will not be liable to prosecution for money laundering offences.

Do not worry that what may be suspicious to you may not be suspicious to another person. Do not be concerned with what someone else might think. If you are in any doubt as to whether circumstances should be reported, you should seek guidance from the MLRO or Legal Department (Legal).

Any Employee who breaches this policy may face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

Anti-Bribery and Corruption

THE LAW

Bribery

Bribery is the offering, promising, giving or accepting of any financial or other advantage, to induce the recipient or any other person to act improperly in the performance of their functions, or to reward them for acting improperly, or where the recipient would act improperly by accepting the advantage.

Financial or other advantage can mean money, gifts, entertainment, travel expenses, holidays, offers of hiring, the award of a contract, discounts, rebates, or charitable or political contributions.

A person acts improperly where they act illegally, unethically, or contrary to an expectation of good faith or impartiality, or where they abuse a position of trust. The improper acts may be in relation to any business or professional activities, public functions, acts in the course of employment, or other activities by or on behalf of any organisation of any kind.

Corruption

Corruption is the abuse of entrusted power or position for private gain.

Many laws prohibit indirect as well as direct corrupt inducement. Accordingly, the Group and its Employees are potentially liable for any prohibited conduct if it is made through any third-party agents, representatives, affiliates, or other intermediaries with the knowledge that a third party will be the ultimate recipient. Knowledge may include conscious disregard or deliberate ignorance (i.e. "turning a blind eye") of facts which indicate a high probability that the corrupt offer, promise or payment will occur.

Many laws specifically prohibit the bribery of public officials. Public officials are a broad category and include persons who you may not normally think of as "public officials", including, potentially, employees of state-controlled commercial entities or investment funds.

Violations can have severe consequences for the Group and for you, including criminal and civil penalties and reputational harm. Any Employee found to have engaged in prohibited conduct or ignored suspicious activity will be subject to disciplinary proceedings, including summary dismissal and/or referral to appropriate law enforcement authorities.

Policy

The Group prohibits bribery and corruption of or by any person or company, in any jurisdiction, wherever they are situated and whether they are a public official or body or private person or company or by any individual Employee, agent or other persons or body on the Group's behalf.

You shall not:

- give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that an improper business advantage will be received, or to reward an improper business advantage already given;
- give or accept a gift or hospitality during any commercial negotiations or tender process, if this could be perceived as intended or likely to influence the outcome;
- accept a payment, gift or hospitality from a third party that you know or suspect is offered with the expectation that it will provide a business advantage for them or anyone else in return;

- accept hospitality from a third party that is unduly lavish or extravagant under the circumstances;
- offer or accept a gift to or from government officials or representatives, or politicians or political parties;
- threaten or retaliate against another individual who has refused to commit a bribery offence or who has raised concerns under this policy; or
- engage in any other activity that might lead to a breach of this policy.

The Group also prohibits facilitation payments which are nominal or routine payments (typically made to low-level government officials) to expedite or secure a service or routine action that these recipients ordinarily perform. They are not common in the UK but are common in some other jurisdictions in which we operate.

Personal funds should not be used, whether directly or indirectly, to accomplish what is otherwise prohibited by this Policy.

The Group prohibits "turning a blind eye" to, or ignoring, suspicious actions on the part of the Group's Employees or third parties as this may result in the Group and the individuals involved being deemed to have knowledge of, or indeed to have assisted, the unlawful transaction.

Giving and receiving Gifts & Entertainment

Gifts and entertainment in particular can be a difficult area because giving a gift or entertainment, although normal industry practice may be construed as an inducement to do something or give the recipient difficulty in acting objectively with respect to the donor.

The Group prohibits the giving or receiving of gifts and entertainment if they are any of the following:

(a) cash or cash equivalents (such as gift certificates, loans, stock, stock options);

(b) unduly lavish;

(c) unreasonable, disproportionate or which goes beyond the standards or norms in the industry;

(d) offered in return for something (rather than being intended only to improve the image of the Group, to better present products and services, or to establish cordial relations). For example, gifts and entertainment must not:

  i. involve parties engaged in a tender or competitive bidding process; or

  ii. be intended to influence the recipient's objectivity in making a business decision; or

  iii. otherwise be intended to influence the recipient to perform a function improperly; or

  iv. be intended to influence a public official in order to obtain or retain any advantage.

(e) be potentially embarrassing to you, the Group, the third party or the third party's organization if it became publicly known;

(f) be potentially unlawful in either your country or the third party's country;

(g) be in breach of the rules or code of ethics of the third party's organization; or

(h) be paid for personally in order to try to avoid these rules.

The Group prohibits solicitation of gifts or gratuities on the basis that it is unprofessional.

Expenses

Reimbursing a third party's expenses, or accepting an offer to reimburse our expenses (for example, the costs of attending a business meeting) would not usually amount to bribery. However, a payment in excess of genuine and reasonable business expenses (such as the cost of an extended hotel stay) is not acceptable.

Donations

We only make charitable donations that are legal and ethical under local laws and practices. No donation must be offered or made over GBP 500 or equivalent without the prior approval of the COO or a member of the Group's Corporate Social Responsibility committee with copy to the COO.

Protection

The Group prohibits and will not tolerate any retribution or retaliation against anyone who has, in good faith, (i) sought advice regarding prohibited conduct (ii) reported a suspicion of prohibited conduct or (iii) refused to participate in prohibited conduct.

PROCEDURE

Reporting Actual or Suspected Wrongdoing

You are required to immediately report to Legal any conduct that you have reason to believe, in good faith, is or may be prohibited conduct and you are not to engage in such conduct.

Prompt reporting and resolution of corruption or bribery issues can help to ensure that we act in accordance with this Code and all applicable laws.

Any report of suspicious conduct will be treated with sensitivity and in confidence to the extent possible. No Group Employee acting in good faith will suffer adverse consequences for reporting or for refusing to engage in prohibited conduct, even if such refusal results in loss of business to the Group.

Internal Financial Controls

We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

You must declare and keep a written record of all hospitality or gifts given, which will be subject to managerial review.

You must declare and keep a written record of all hospitality or gifts received which exceed GBP 1000, which will be subject to managerial review.

You must submit all expenses claims relating to hospitality, gifts or payments to third parties in accordance with our expenses procedure and record the reason for expenditure.

All accounts, invoices, and other records relating to dealings with third parties including suppliers and customers should be prepared with strict accuracy and completeness. Accounts must not be kept "off-book" to facilitate or conceal improper payments.

Breaches of this Policy

Any Employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

Finally, the Group recognises that sometimes judgments have to be made by Group personnel as to the appropriateness, or otherwise, of conduct or proposed conduct. The Group very much encourages a culture where you feel free to consult with your MD before making decisions. If in doubt – ask.

Sanctions

The Law

The UK, the US, the European Community (EU), the United Nations Security Council and individual countries sometimes impose economic sanctions and embargoes restricting their nationals, corporations and, in some cases, foreign subsidiaries, from doing business with certain countries, legal entities and/or individuals including organizations associated with terrorist activity and narcotics trafficking.

These sanctions vary from country to country but at their broadest prohibit business dealings of any nature with targeted governments and organizations, as well as individuals and entities that act on their behalf. Sanction prohibitions also may restrict investment in a targeted country, as well as trading in goods, technology and services with a targeted country. A UK, US, EU or other person also may not be permitted to approve or facilitate transactions by using a third party not subject to those sanctions if they themselves could not transact directly.

As of January 2023, the following countries were targeted by certain types of sanctions (the "sanctioned countries"). Please check the Compliance tab in the Group directory for an up to date list of countries subject to sanctions:

Afghanistan	**Belarus**	**Cuba**	**Central African Republic**	**China**	**Zimbabwe**
Democratic Republic of the Congo	**Eritrea**	**Haiti**	**Iran**	**Iraq**	**North Korea (DPRK)**
Lebanon	**Libya**	**Myanmar (Burma)**	**Russia**	**Somalia**	**Sudan**
South Sudan	**Syria**	**Ukraine**	**Venezuela**	**Yemen**	

The sanctions vary from country-to-country and, in many of the listed countries, the sanctions are limited to those against named organisations, entities or individuals (known as Specially Designated Nationals under the US regime). In addition to targeting countries, embargoes or sanction laws may restrict or prohibit business by their nationals with certain specific entities and individuals, wherever they may be located (Prohibited Persons under US regime).

The exact requirement of UK sanctions relating to any country contained on the above are summarized at https:// www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets and https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation are subject to change.

The exact requirement of EU sanctions relating to any country contained on the above are summarized at https://www.eeas.europa.eu/eeas/european-union-sanctions_en and are subject to change.

The exact requirements of US sanctions relating to any country contained on the list above are summarized at https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information and are subject to change.

The consequences of breaching sanctions are severe and include punitive fines, imprisonment, criminal proceedings, reputational damage and sanctioning.

Policy

The Group is committed to compliance with relevant economic and trade sanctions laws in all jurisdictions in which it operates, is registered and/or licensed.

Under no circumstances may an Employee breach sanctions or evade detection of a transaction in breach of this policy. The Group and its Employees must not advise clients on how transactions should be structured or presented in order to avoid detection of a breach of applicable sanctions. For example, they cannot advise clients to amend their instructions to include details that are false or misleading, or change, remove or omit information from a transaction that would otherwise lead to detection of a breach.

Procedures

The Group provides sanctions notifications and training to relevant Employees and Legal provides guidance and oversight.

The Group screens for designated entities and sanctioned countries in accordance with applicable sanctions regimes in the UK and overseas using an in-house checking tool known as “Client Check” found on the Group directory. Employees have been instructed on how to use this tool.

Employees must remain vigilant to ensure compliance with this policy. If an Employee suspects a breach or potential breach of the Group’s obligation under this policy, they must report it to Legal.

We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

Because sanctions are subject to change, it is vital that Employees consult the most recent version of these sanctions if there is any question about the ability to do business with a client or in a country and consult first with Legal. Legal should always be notified when dealing with any business or individual connected to the countries on the list.

Any Employee who breaches this policy may face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

Anti-Competitive Behaviour/ Market Manipulation

The Law

Competition or antitrust laws differ from country to country. Anti-competitive behaviour can occur when illegal cooperation takes place between competitors. It can also occur if Employees facilitate or enable coordination between customers where such coordination has the object or effect of restricting, preventing or distorting competition.

Violations of competition laws can result in punitive fines, criminal prosecution, imprisonment and reputational damage both for the Group and for individuals.

Policy

The Group supports free competition and opposes any form of unfair business monopolies, such as cartels. Employees must NOT:

- participate in any discussion or enter into any agreement which has the object or effect of restricting, preventing or distorting competition;
- share with one customer information that could be used by that customer to determine the prices or commercial strategy of another customer;
- deliberately disseminate incorrect or misleading price information;
- discuss details of business terms with any customer in the presence of other customers or competitors;
- act as a conduit for the flow of confidential commercial information from one customer to another and/or facilitate such a flow of information where such coordination has the object or effect of restricting, preventing or distorting competition;
- engage in any agreements or arrangements with any competitors:
  - (i) to fix, stabilize or raise market prices or profit margins;
  - (ii) to fix the price or terms and conditions of market bids;
  - (iii) to reduce market output;
  - (iv) to refrain from dealing with certain clients with the object of restricting, preventing or distorting competition;
  - (v) to refrain from competing for certain bids; or
  - (vi) to refrain from competing in certain geographic areas or markets;
- discuss or exchange information with any competitors on prices, business expansion plans or marketing plans;
- associate with any discussions, meetings or activities appearing to constitute anti-competition and you must record in writing that you did not participate in those events;
- ask your customers to provide information as to what your competitors are doing on a regular basis.

Procedure

All Employees should contact Legal if they have any concerns as to whether a proposed contractual arrangement may breach this policy.

All Employees must promptly report to Legal any violations or suspected violations by Employees or others doing business on the Group's behalf.

Any Employee who breaches this policy may face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

Facilitation of Tax Evasion

The Law

Under English law, a company is guilty of an offence of facilitating tax evasion if a person acting for the company (whether employee, contractor or agent) facilitates UK or foreign tax evasion.

In order to facilitate such tax evasion, the employee, contractor or agent must be knowingly concerned in or take steps with a view to facilitating the fraudulent evasion of a tax by another person or must aid, abet, counsel or procure the tax evasion.

The offence is only committed where Employees, contractors or agents deliberately and dishonestly take action to facilitate UK tax evasion or foreign tax evasion. However, a deliberate failure to report suspected tax evasion or foreign tax evasion, or "turning a blind eye" to suspicious activity could amount to criminal facilitation of tax evasion.

A company guilty of an offence of failing to prevent facilitation of tax evasion is liable to unlimited fines as well as exclusion from tendering for public contracts and damage to its reputation. We therefore take our legal responsibilities seriously.

It is a defence for the Group to prove that at the time the facilitation offence was committed, it had in place such prevention procedures as it was reasonable in all the circumstances to have in place.

Policy

The Group takes a zero-tolerance approach to tax evasion. Employees must not engage in any form of facilitating tax evasion, whether under UK law or under the law of any foreign country.

Employees must at all times read, understand and comply with this policy which is also available on the intranet.

Employees in treasury and finance, in particular, are required to read, understand and comply with the KYC Manual and Payaways Training Manual.

It is not acceptable for Employees (or someone on their behalf) to:

(a) engage in any form of facilitating tax evasion or foreign tax evasion;

(b) aid, abet, counsel or procure the commission of a tax evasion offence or foreign tax evasion offence by another person;

(c) fail to promptly report in accordance with this policy any request or demand from any third party to facilitate the fraudulent evasion of tax (whether UK tax or tax in a foreign country), or any suspected fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, e.g. such as a request by a supplier to be paid in cash;

(d) engage in any other activity that might lead to a breach of this policy; or

(e) threaten or retaliate against another individual who has refused to commit a tax evasion offence or a foreign tax evasion offence or who has raised concerns under this policy;

The prevention, detection and reporting of tax evasion and foreign tax evasion are the responsibility of all those working for the Group or under its control. Employees are required to avoid any activity that might lead to, or suggest, a breach of this policy.

Procedure

Employees must immediately report to Legal or MLRO any request or demand from a third party to facilitate the evasion of tax, or any concerns they may have that such a request or demand may have been made.

If Employees are unsure about whether a particular act constitutes tax evasion or foreign tax evasion, they must raise it with Legal or MLRO as soon as possible.

Training on this policy forms part of the induction process for all finance and treasury individuals who work for the Group, and such training is embedded in the wider AML detection and prevention training.

Any Employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

The Group may terminate its relationship with other individuals and organisations working on its behalf if they breach this policy.

Whistleblowing Policy

This policy applies to all employees and contractors ("Employees") employed by the Clarksons Group of companies. The policy outlines the process for reporting suspected misconduct, illegal acts or failure to act within applicable internal rules and policies by Employees.

What you should report

If Employees have any concerns during their employment that:

(a) any criminal offence has been or might be committed;

(b) a legal obligation is not being met by the Group or that any malpractice is being committed by the Group or any of its clients, customers or other third party;

(c) there are health and safety risks to themselves, other Employees or the public at large that having been reported to the Group's health and safety representative, have not been adequately dealt with;

(d) any violation of Information security policies or procedures has been or might be committed;

(e) any violation of the Compliance Manual or procedures has been or might be committed;

(f) any person is attempting to conceal evidence relating to any of these matters;

(g) discrimination based on sex, sexual orientation, race, religion, physical disability, age or other factors and sexual harassment in any form;

Then the Employee should raise their concern immediately with the relevant person.

To whom you should report

The person to whom you should report your concerns will depend on the type and seriousness of the alleged wrongdoing:

(a) Should normally report your concerns to your MD or Group COO (Jeff Woyda) subject to (b), (c) and (d) below.

(b) All criminal offences including corruption, money laundering, fraud, market manipulation, sanctions violations or material breaches of applicable laws should be reported to the Group GC (Sandra Rosignoli) or Legal or Group COO (Jeff Woyda).

(c) Violations of information security policies should be reported to the Group CSO (Richard Wright).

(d) If your office has its own local mandatory Whistleblowing Policy, you should follow the reporting procedures in your local policy. Any such local mandatory Whistleblowing Policies are available in the compliance tab in the directory.

(e) If either the Group GC or Group COO are involved, you may contact the Group CEO (Andi Case) or the Group chair of the audit committee (Susan Harris) on her email address Susan.Harris@clarksons.com.

Employees concerned about speaking to another member of staff within the Group can speak, in confidence, to an independent external whistleblowing line managed by Safe Call, by calling the numbers below or filing an on-line report at www.safecall.co.uk/report. Your concerns will be reported to Clarksons without revealing your identity if you request anonymity.

Country	Phone Number
Australia	1800 312928
Brazil	0800 892 1750
Canada	1877 59 98073
China	10800 7440605 China Unicom/ Netcom
China	10800 4400682 China Telecom
China (Shared Cost)	4008 833405
Denmark	00 800 72332255
Egypt	0800 000 0059
Germany	00 800 72332255
Greece	00800 44141966
Hong Kong	3077 5524
India	000 800 4401256
Italy	00 800 72332255
Japan	0120 921067

Country	Phone Number
Morocco	8000 96071
Netherlands	00 800 72332255
Norway	00 800 7233 2255
Korea, South	001 800 72332255 Korea Telecom
Korea, South	001 800 72332255 Dacom
Russia	810 800 72332255
Singapore	800 4481773
South Africa	0800 990243
Spain (inc. Canary)	00 800 72332255
Sweden	0850 252 122
Switzerland	00 800 72332255
UAE	8000 4413376
UK	0800 9151571
USA	1 866 901 3295

How to raise a concern or report a concern

You may raise your concern by telephone, in person or in writing. Please include as much information as possible about the perceived misconduct. When raising a concern, you will need to provide the following information:

- The nature of your concern and why you believe it to be true.
- The background and history of the concern (giving relevant dates).

You will need to demonstrate that you have a genuine concern relating to suspected wrongdoing or malpractice and there are reasonable grounds for your concern.

Actions from Clarksons

We will respond to your concerns as soon as practically possible. In order to be fair to all Employees, including those who may be wrongly or mistakenly accused, initial enquiries will be made to decide whether an investigation is appropriate and, if so, what form it should take.

The investigation may need to be carried out under terms of strict confidentiality, i.e. by not informing the subject of the complaint until (or if) it becomes necessary to do so in the discretion of Clarksons.

Where appropriate, the matters raised may:

- Be investigated by management or external experts such as lawyers or special investigators.
- Be referred to the police.
- Be referred to the external auditor.
- Form the subject of an independent inquiry to regulatory authorities or other governmental authorities.

Employees, who have raised concerns internally, will be informed of who is handling the matter, how they can make contact with them and if there is any further assistance required.

Employees' identities will not be disclosed without prior consent. Where concerns are unable to be resolved without revealing the identity of the employee raising the concern, (e.g. if their evidence is required in court), we will enter in to a dialogue with the employee concerned as to whether and how we can proceed.

THE WHISTLEBLOWER

Anonymous Allegations

You may raise your concerns anonymously; however it will be more difficult for us to protect your position, investigate the matter at hand or give feedback.

Concerns expressed anonymously may be considered at our discretion considering the seriousness of the issue raised, credibility of the concern and the likelihood of confirming the allegation from other sources.

Untrue Allegations

If the event you make an allegation in good faith and reasonably believe it to be true however the investigation confirms that the matter or allegation is untrue or immaterial, we will recognize your concern and not take any actions against you. In the event any employee or contractor make an allegation frivolously, maliciously or for personal gain, appropriate actions will be considered by Clarksons against the reporting person that may include disciplinary action.

Whistleblower Protection

The Group prohibits and will not tolerate any retribution or retaliation against any Employee who raises a concern in good faith in accordance with this policy and such Employee shall not be victimised or penalised in any way for raising their concern.

In the event that you believe that you are being subjected to a detriment by any person within the Group as a result of your decision to invoke this procedure you must inform the person to whom you have whistle blown immediately and appropriate action will be taken to protect you from any reprisals.

Last revised January 2023