



M GROUP

# Financial Crime Procedure

## Financial Crime Procedure

MGS-PRO-LEG-001

01 July 2025



# Contents

1.	Introduction	4
2.	Purpose	4
3.	Scope	4
4.	Bribery	4
5.	Gifts and Hospitality	5
6.	Corruption	6
7.	Conflicts of Interest	6
8.	Fraud	8
9.	Anti-Money Laundering	9
10.	Trademark and Economic Sanctions	9
11.	Corporate Criminal Offences	10
12.	Raising a Concern	10

When changes affect a considerable number of pages, this document shall be re-issued/revised in its entirety, incorporating all previous revisions. A number shall identify issues and each issue shall cancel and replace all previous issues and revisions. Revisions shall be identified by a number and shall replace the previous revision.

Revisions shall be notified to relevant M Group companies' employees through an internal memorandum or other appropriate form of communication.

---

<b>Date</b>	<b>Version</b>	<b>Owned By</b>	<b>Changes</b>
<b>15/10/2024</b>	v1.0	Alex Badel	<b>New document</b>
	v1.1	Alex Badel	<b>Updated to reflect new failure to prevent fraud offence introduced by Economic Crime and Corporate Transparency Act 2023</b>
<b>22/07/2025</b>	V1.2	Alex Badel	<b>Updated to introduce de minimis value for gifts and hospitality of £20 and additional information regarding conflicts of interest</b>

## 1. Introduction

- 1.1 This Financial Crime Procedure describes how M Group (Services) Limited and its group companies (“we”, “our”, “us”, “the Group”) approach financial crime which encompasses bribery, corruption, fraud, money laundering, sanctions and corporate criminal offences.
- 1.2 We are committed to acting professionally, honestly and with integrity in all business dealings and, as such, have a zero-tolerance approach to any form of financial crime or corrupt activity.

## 2. Purpose

- 2.1 The purpose of this Financial Crime Procedure is to set out what is, and is not, acceptable to ensure our compliance with all laws relevant to countering financial crime in the United Kingdom. Failure to adhere to this Procedure may lead to disciplinary action against employees including dismissal and/or termination of relationships with others, such as third-party service providers. It may also result in criminal prosecution, fines and imprisonment.
- 2.2 Failure by any employee to report a financial crime or corrupt activity by other persons may also result in disciplinary sanctions, especially where there is evidence that an employee has attempted to cover up or disguise another’s wrongdoing.

## 3. Scope

- 3.1 This procedure applies to all employees, workers, agency staff, contractors, third parties and supply chain partners who perform services for and on behalf of the Group. This includes all company operations, activities and transactions and, in addition to this procedure, all parties are expected to abide by the ethical standards and requirements set out in our [Governance framework](#) (link).

## 4. Bribery

- 4.1 The Bribery Act 2010 defines bribery as offering, promising, giving, receiving or soliciting something of value to influence an action or decision. A bribe may be made directly or indirectly i.e. to someone else other than the person who is to be influenced.
- 4.2 The Bribery Act 2010 creates five offences:
  - 4.2.1 offering to or giving a bribe to another;
  - 4.2.2 accepting or requesting a bribe;
  - 4.2.3 bribery of a foreign (non-UK) public official;
  - 4.2.4 consent (active or passive) by a director or senior company officer in bribery by a company; and
  - 4.2.5 failure by a commercial organisation to prevent bribery on its behalf by its associated persons.
- 4.3 The consequences of infringing the Bribery Act 2010 are extremely serious for individual employees, the Group and other stakeholders. Offences carry a penalty of a fine or 10 years imprisonment (or both) for individuals found guilty and an unlimited fine for an offence of failing to prevent bribery under paragraph 4.2.5 above. In addition, the Group would face exclusion from tender opportunities and suffer serious reputational damage.
- 4.4 To ensure that no offence is committed by any party acting for or on behalf of the Group, we must adhere to the following requirements:
  - 4.4.1 Facilitation Payments: These are typically small, unofficial payments made to speed up an administrative process or secure a routine government action by a public or government official. Facilitation payments are illegal under UK law and so are strictly prohibited.
  - 4.4.2 Political Donations: The Group’s funds and resources are not to be used to contribute to any political campaign, political party, political candidate or any of their affiliated organisations.
  - 4.4.3 Charitable Donations: Charitable donations may only be made in accordance with the Group Charitable Giving and Volunteering Policy, which is available from Group Finance.
  - 4.4.4 Cash Payments: No payments to any other party may be made in cash.

## 5. Gifts and Hospitality

- 5.1 Gifts include any item of value provided to a third party or their employees or received from a third party by us or our employees.
- 5.2 Hospitality includes any business entertaining, such as travel, accommodation, meals and invitations to events given to the Group and its employees by third parties or given by the Group to third parties.
- 5.3 We discourage employees from accepting or giving gifts or hospitality. We accept that modest gifts and corporate hospitality can generate goodwill, legitimately promote products and services, and improve working relationships. However, it is essential that they do not influence, nor could be perceived as influencing, business decision making. This procedure therefore allows for the giving or receiving of reasonable and appropriate gifts and hospitality for the following purposes:
- 5.3.1 establishing or maintaining good business relationships;
  - 5.3.2 attending relevant conferences, industry events or training sessions;
  - 5.3.4 improving or maintaining our image or reputation; or
  - 5.4.5 marketing or presenting our products and/or services effectively.
- 5.4 The giving or receiving of gifts and hospitality for one of the above purposes must be carried out in accordance with the following requirements to ensure interactions are transparent and safeguard against the risk that any gift or hospitality could be construed as a bribe:
- 5.4.1 Gifts and hospitality must be given and received openly, to all relevant parties in a non-discriminatory manner, to cement good relations and not show any intent to induce improper performance from another party, influence decision making or compromise professional judgement;
  - 5.4.2 Conversely any gift or hospitality which is offered to an employee of the Group must not be accepted if the intent of the giver is that the employee will take actions which are not in good faith or in accordance with the position of trust held by the employee and such that the employee and the Group is compromised, potentially compromised or could be perceived as being compromised as a result;
  - 5.4.3 We should not request or solicit gifts or hospitality. It is not appropriate to solicit funding, goods or services from suppliers, subcontractors or other third parties for personal use, team events, or for internal functions or other events (charitable or otherwise), for example, the provision of items for raffles or draws. Should suppliers or subcontractors wish to support charitable events in which the Group is involved then this should be provided by the third-party making direct contact with the organisation that is fundraising. The Group should not act as a conduit for such support;
  - 5.4.4 Gifts should be of a modest value and appropriate for the context. For example, promotional gifts of low value such as branded stationery to or from existing customers, suppliers and business partners will usually be acceptable;
  - 5.4.5 Gifts valued less than or equal to £20 do not need to be recorded on the Gift and Corporate Hospitality Register. Gifts valued greater than £20 and less than or equal to £50 must be approved by an individual's Line Manager. Any gift valued at more than £50 must be approved by an Executive Team member (Divisional Managing Director, or Group Executive member) in advance. For how to do this, see paragraph 5.5 below;
  - 5.4.6 Gifts must never be given to a public official;
  - 5.4.7 Hospitality must not come with lavish 'add-ons' such as for inappropriate travel and accommodation costs; and
  - 5.4.8 Hospitality valued less than or equal to £20 does not need to be recorded on the Gift and Corporate Hospitality. Hospitality valued greater than £20 and less than or equal to £300 per individual must be approved by an individual's Line Manager in advance. Hospitality greater than £300 per individual

must be approved by an Executive Team member (Divisional Managing Director, or Group Executive member) in advance. For how to do this, see paragraph 5.5 below.

### **Declaring Gifts and Hospitality**

- 5.5 All gifts and hospitality valued greater than £20 must be accurately recorded on the Gift and Corporate Hospitality Register before being offered to/ accepted from someone. This can be accessed via your Oracle account (accessed in the same location and with the same details as you would use to find payslips, book leave etc.), where a 'Gifts and Hospitality icon' will be visible. By completing the information using this icon, this submits the request to the Gift and Corporate Hospitality Register and to the relevant individual for approval. The gift/hospitality must not be given, or accepted, until you have received the confirmation that it has been approved.
- 5.6 On a quarterly basis, a list of gifts and hospitality will be shared with the Divisional Risk Management Committee to review this for its reasonableness and completeness.

## **6. Corruption**

- 6.1 Corruption is the abuse of an entrusted power or position for private gain. The UK Bribery Act makes all forms of corruption illegal and as such the Group strictly prohibits it.
- 6.2 The risks of corruption are not always obvious. Accordingly, we must all, including all parties acting on behalf of the Group, adhere to the following:
- 6.2.1 Not to make payments to someone (or favour them in any other way) if you know this will involve them misusing their position or performing their function improperly;
  - 6.2.2 Not to misuse your position (or perform your function improperly) in connection with payments (or other favours) for yourself or others;
  - 6.2.3 If in doubt, do not proceed with the payment or transaction and seek further guidance; and
  - 6.2.4 If anyone acting on behalf of the Group needs to promote the company's business with a foreign public official, or someone working at an overseas publicly owned organisation, this must be checked in advance with the Group General Counsel.

## **7. Conflicts of Interest**

- 7.1 A conflict of interest is a situation in which a person or organisation has two or more competing interests which impairs their ability to make objective, unbiased business decisions. For instance, a conflict may arise if our professional duties as an employee and our personal interests diverge.
- 7.2 The requirements of this policy extend to conflicts of interest that are:
- 7.2.2 actual, potential or perceived; and
  - 7.2.2 personal or organisational.
- 7.3 It is best practice to avoid not only actual or potential conflicts but also the perception of a conflict. We have to think about how a situation may look to someone else. Whilst there may be nothing improper happening, it is better to avoid even the idea of a conflict and to take steps to address the issue rather than having to undergo a time consuming investigation to prove there was no conflict.
- 7.4 To ensure independence and judgement is not compromised, we must adhere to the following requirements.

### **Personal Conflicts**

- 7.5 Employees and parties working on behalf of the Group must ensure no conflict, or the appearance of a conflict, exists between their personal interests and the interests of the company.
- 7.6 Personal interests also include the interests of an individual's close family members (including children, parents, partner, civil partner or spouse, common law spouse, in-laws or other individuals who, in the reasonable opinion of M Group, could be considered as falling within this category).

- 7.7 People and parties working on behalf of the Group must not use their position, status, or contacts within the Group to attempt to influence decisions that would benefit a close family member.
- 7.8 Examples of personal conflicts include:
- 7.8.1 one of our people or their close family member having an interest, dealings or shareholding in a client, competitor, subcontractor, supplier or partner of M Group (or is seeking to become one);
  - 7.8.2 one of our people procuring works, materials or services from an M Group subcontractor or supplier for their own personal use;
  - 7.8.3 one of our people arranging for M Group, an M Group subcontractor or supplier, to provide works, materials or services to a client or potential client for their personal use;
  - 7.8.4 one of our people who has a close family member working in M Group or is directly recruiting a close family member to a position in M Group.
- 7.9 As such, we must not do any of the following for our own personal benefit or the benefit of a close family member:
- 7.9.1 attempt to influence Company decisions;
  - 7.9.2 give preferential treatment to any party;
  - 7.9.3 use Company resources (including materials, premises, plant, supplies or the services of other employees/associated persons of the Company);
  - 7.9.4 benefit directly or indirectly from a business transaction.
- 7.10 Further, any directorship or shareholding greater than 5% in any party must be declared using the process below. Approval from the Managing Director of the Division must be in place prior to the Group entering into any contract of any kind with this party.

### **Organisational Conflicts**

- 7.11 A conflict of interest can also occur where the involvement of one of our people, an M Group team, department or entity gives rise to an actual or perceived unfair benefit or hindrance to M Group's corporate interests or those of a client, supplier or partner.
- 7.12 For example, where the Group has provided advisory services in the early design stage of a project, this may create an unfair advantage (or perception of an unfair advantage) if the Group was to competitively bid for the construction phase of the same project. In these circumstances, the Procurement Act 2023 provides that a Contracting Authority may exclude the supplier from the procurement process if the advantage cannot be avoided.
- 7.13 Another example is where the Group appointed an adviser to support with the preparation of a bid for a client and the same advisor was also appointed by the client to support the client with the same procurement exercise. These circumstances could also result in the exclusion of the Group from the procurement process.

### **Declaring Conflicts**

- 7.14 All actual or potential conflicts must be declared on the Conflicts of Interest register, which can be accessed via your Oracle account (accessed in the same location and with the same details as you would use to find payslips, book leave etc.), where a 'Conflicts of Interest icon' will be visible. By completing the information using this icon, this submits the request to the Conflict-of-Interest Register and to the relevant individual (Divisional Managing Director or Group Executive member) for approval. They will either approve the interest with no additional action required or state conditions that must be met to ensure no conflict arises. This could include removing the individual from being involved in making decisions where a conflict could arise, altering the hierarchical structure or removing the individual from a particular project where a conflict could arise. The decision of the Managing Director or Group Executive member will be shared with the individual, and their Line Manager, who must then confirm that this has been actioned.

## Managing a Conflict of Interest

- 7.15 When considering how to manage or remove a conflict of interest, please consider one or more of the following steps:
- 7.15.1 Ring fencing individual employees or teams that have knowledge or information that gives rise to a conflict by:
- a) Creating distinct and separate reporting lines and supervision arrangements;
  - b) Using isolated and secure firewalls, restricted access, password protection and data encryption;
  - c) Ensuring employees or teams operate from different physical locations,
- 17.15.2 Requiring employees to remove themselves from any decision-making process or actions related to the conflict of interest;
- 17.15.3 Requiring employees to divest themselves of any shareholding or interest in any company with which there is a conflict of interest;
- 17.15.4 Requiring employees to refrain from engaging in any activity that may create or appear to create a conflict of interest;
- 17.15.5 Use of non-disclosure agreements to confirm that all information held in relation to a project or activity will be held confidentially and not disclosed to anyone working outside of the project or activity team; and/or
- 17.15.6 Putting in place a 'Conflict of Interest Plan' or 'Separation Protocol' specific to the project or bid where the conflict has arisen setting out the measures that will be put in place and reported on to the client on a regular basis.
- 17.16 Once identified, the solution should be recorded in on the Conflicts of Interest register and implemented. If there needs to be a change to the solution or the nature of the conflict of interest alters, then this can be considered and the solution amended as appropriate. For guidance on identifying and implementing solutions to conflicts of interest, please contact the Group General Counsel.

## 8. Fraud

- 8.1 Fraud is a serious criminal offence, which can be defined as any intentional act or omission designed to deceive others resulting in the victim suffering a loss and/or the perpetrator achieving a gain. Examples of fraud offences include:
- 8.1.1 Fraud Act 2006: dishonest false representations or omissions made for gain;
- 8.1.2 Theft Act 1968: false accounting, false statements made by directors;
- 8.1.3 Companies Act 2006: fraudulent trading;
- 8.1.4 Scottish Common Law: embezzlement (stealing money or assets from an employer or business), uttering (using a forged document with the intent to defraud);
- 8.1.5 cheating the public revenue.
- 8.2 Fraud has the potential to harm our business, and create financial loss, and so the Group has a zero-tolerance approach to fraud. This means that all fraudulent activity is prohibited, and any concerns that fraudulent activity is taking place should be reported immediately in accordance with our [Whistleblowing Policy](#).
- 8.3 The following are examples of fraudulent activity:
- 8.3.1 Forgery or alteration of documents (timesheets, invoices, bank accounts etc.);

- 8.3.2 Misrepresentation of information on documents;
  - 8.3.3 Misappropriation of funds, supplies or assets;
  - 8.3.4 Theft, disappearance or destruction of assets;
  - 8.3.5 Authorising or receiving payment for hours not worked;
  - 8.3.6 Disclosing confidential information to outside parties;
  - 8.3.7 Claiming expenses that are not genuine or not in line with the [Expenses Policy](#);
  - 8.3.8 Improprieties in the handling or reporting of money or financial transactions.
- 8.4 Any person committing a fraud may be criminally prosecuted facing fines and/or imprisonment. In addition, an organisation that fails to prevent fraud from which it benefits may now be prosecuted.
- 8.5 A new offence for failing to prevent fraud has been introduced as part of the [Economic Crime and Corporate Transparency Act](#) (ECCTA) taking effect from 1 September 2025. The new offence applies to large organisations which are businesses with at least two of the following criteria applying: more than a £36m turnover; more than £18m in assets; more than 250 employees.
- 8.6 The offence applies if an associated person of the Group commits a fraud with an intention to benefit the Group (or any part of the Group) or an organisation to which the associated person provides services to (i.e. a client). An associated person includes directors, officers, employees, agents and subsidiary companies within the Group or other persons who perform services for or on behalf of M Group.
- 8.7 An associated person is not limited to the most senior director and officers. Under ECCTA, the scope has been significantly expanded to include “senior management” which includes:
- 8.7.1 an individual who plays a significant role in:
    - a) the making of decisions about how the whole/ substantial part of the business are to be managed or organised, or
    - b) the actual managing or organising of the whole/substantial part of those activities.
- 8.8 The above may apply to regional managers or managers of an operational part of the business. As such if a senior manager of M Group acting within the actual or apparent scope of their authority commits a fraud offence, M Group may also be guilty of an offence.
- 8.9 The Group has a Fraud Risk Framework, which can be provided as needed from the Group Head of Risk and Business Continuity. This sets out the Group’s approach to preventing and detecting fraud and is supported by a detailed fraud risk assessment that has been completed by all Divisions, and Group Support functions. The output of the risk assessment is recorded on Xactium, the Group’s risk management tool, alongside the controls in place to mitigate the identified risks. This is shared annually with the Risk Board and our external auditors.
- 9. Anti-Money Laundering**
- 9.1 We should be mindful of any activity that could potentially be money laundering (e.g. clients over-paying and requesting refunds, requesting payment into a different bank account to the usual account and/or asking for payment to a non-UK bank account). Money laundering is the process that turns the proceeds of criminal activity into funds that appear lawful and is illegal under the Proceeds of Crime Act 2002.
- 9.2 Whilst the Group is not a high-risk organization for money-laundering, we must ensure that appropriate due diligence is completed on all parties that we engage with. For guidance on what is required to carry out appropriate money-laundering checks, please contact the Group General Counsel. Any suspicious activity must be reported immediately using the [Whistleblowing Policy](#).
- 10. Trademark and Economic Sanctions**

10.1 The UK sanctions regime imposes serious and extensive restrictions on dealing with people who are listed ('designated persons'), such that even legitimate payments cannot be made to them. The Group must adopt an appropriate risk-based approach to ensure that the UK sanctions regime is complied with. This will include periodic checking of suppliers, subcontractors and employees against the sanctions list, including before engaging them. Any matches, or close matches, must be reported to the Group General Counsel immediately and no payments made to that individual, or entity, until advice has been received from the Group General Counsel.

## 11. Corporate Criminal Offences

11.1 The Criminal Finances Act 2017 introduced two Corporate Criminal Offences (CCO):

11.1.1 the failure to prevent facilitation of UK tax evasion, and

11.1.2 the failure to prevent facilitation of foreign tax evasion.

11.2 The legislation concerns businesses such as ours being able to demonstrate we can prevent the facilitation of tax evasion as part of our day-to-day operations. Specifically, the legislation means that if an 'associated person' of a business does criminally facilitate tax evasion, and the business is unable to demonstrate that it had reasonable procedures in place to prevent such facilitation, the business is guilty of a criminal offence.

11.3 An 'associated person' is defined as a person who performs services for or on behalf of our organisation. This can be an individual or an incorporated or unincorporated body. Typically, this includes suppliers, agency workers, outsourced service providers, contractors etc. The CCO requirements also apply to all our employees in how they manage their relationships with anyone they meet during the course of working for us, and this will include actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

11.4 The consequences of a prosecution for the business include unlimited fines, reputational damage and the likelihood of regulatory sanction. Tax evasion and facilitation of tax evasion are also punishable for individuals with fines and custodial sentences. We therefore take our legal responsibilities very seriously. Any individual who breaches this policy may face disciplinary action, potentially resulting in dismissal for misconduct or gross misconduct. Similarly, we may terminate our relationship with other individuals, organisations and other associated persons working on our behalf if they breach this policy.

11.5 The legislation applies to all taxes – personal and corporate tax – and includes other taxes such as VAT, Customs Duties, National Insurance Contributions etc.

11.6 Training is provided to staff in relevant roles and regular risk assessments are completed. In addition, all our people and parties acting for or on behalf of the Group must not:

11.5.1 Undertake any transactions which could commit tax evasion.

11.5.2 Facilitate tax evasion by a third party.

11.7 If there is anything unusual about the way a person associated with the Group is behaving, or conducting business with us, please seek further guidance from the Group Head of Tax.

## 12. Raising a Concern

12.1 If you have any concern about anyone who is or may be committing a financial crime, whether it be bribery, corruption, fraud, money laundering, breach of sanctions or any corporate criminal offence, you should act promptly by raising the issue with your line manager, the Group Director of Internal Risk and Audit or the Group General Counsel so it can be investigated as soon as possible.

- 12.2 An independent whistleblowing hotline is available, operated by Navex. Reports can be made via a call, where an independent call agent will record your concerns, or via an online form, anonymously where required, as per the below:



Dial: 0-800-89-0011 (British Telecom)

Then dial: 833 573 1738

<http://mgroupservices.ethicspoint.com/>