Third-Party Speak-Up Policy

1. Introduction

This Third-Party Speak-Up Policy ("Policy") is intended to encourage and enable business partners and their respective employees as well as other third parties (Suppliers, Contractors or Sub-contractors) to report concerns and suspected breaches of relevant legislation.

2. Who this applies to

This policy applies to IMG (UK) Holdings Limited, its subsidiary entities, and those companies connected through common ultimate ownership (IMG)[1] and its suppliers for goods and services, Business Partners and respective employees known as ("**Reporters**").

3. General Principles

Notwithstanding the circumstances under which a report is made, IMG adheres to and will apply the following principles to all situations and measures undertaken.

Examples where it may be necessary to report a concern, included but not limited to:

- Bribery & Corruption
- Theft
- Modern Slavery
- Abuse of Power
- Bullying, Aggression, Harassment or Discrimination
- Safeguarding
- Health & Safety
- Behaviour/Cultural Issues
- Regulation/Legislation Breach
- Other, Unethical or Improper Conduct

3.1. Protection of Reporters

IMG believe that the functionality of third-party reporting on violations can only work following a transparent and trustworthy process in which Reporters are aware that they act in a safe and protected environment.

We therefore commit to the following principles:

- **Non-retaliation**: Reporters do not have to fear negative consequences of discriminatory or disciplinary nature for making a report in good faith or raising questions, doubts and concerns.
- **Fair**: All cases will be subject to strict impartiality; the assumption of innocence applies and the right to be heard apply is granted.
- **Confidentiality:** We will undertake all reasonable efforts to preserve the

[1] *List of Active & Dormant Companies | IMG*

confidentiality of legitimate reporting and the information contained therein the widest extent possible. Therefore, reports can also be submitted anonymously.

IMG reserves the right to make disclosures if:

- The Reporter has consented.
- There is a requirement for effectively investigating the report and taking related measures.
- The necessity for compliance with a mandatory legal obligation.
- The disclosure is mandatory under applicable law.

3.2. Exception for Misuse

Intentionally misusing the reporting system under this Policy for abusive practice (i.e., filing reports in bad faith or as an act of revenge) is strictly prohibited. Reporters who use the reporting system in an abusive way are not protected by the principles set above and may find themselves guilty of an offence. We do not tolerate any kind of threats, detrimental behavior or acts of retaliation. Such conduct is a breach of our values and may result in legal action being considered.

3.3 Informing concerned Individuals

IMG will inform the persons concerned that a report has been made, where it is necessary to assist in the investigation.

Depending on the specifics of each case, we may withhold certain information to avoid compromising the investigation, protecting evidence, or the reporting process.

3.4 Data Protection

When handling reports, we are dedicated to protecting the confidentiality and privacy of information entrusted to us in accordance with the UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018. The Data Protection regulations in both Europe and UK shall apply as we have offices based in these locations.

Records of reports and the related investigation materials will be stored in accordance with the retention policy and to the extent this is necessary for the achievement of IMG's legitimate interest, in particular the operation of the internal reporting channels and an effective compliance management. Other legitimate interests include the establishment, exercise or defense of legal claims or ensuring compliance with applicable statutory obligations to which we are subject to. Records will be deleted in accordance with applicable data protection laws.

Unverified reports or information deemed beyond the scope of this Policy will be immediately deleted in compliance with applicable laws and regulations.

4. Reporting Procedure and Case Management

The reporting procedure under this Policy is built to allow an efficient, secure and transparent handling of reports.

Reporters can support this ambition by providing information in a concise and sufficiently detailed manner, including supporting evidence where available.

4.1 Reporting and Follow-Up

Reports can be brought to IMG via one of the following reporting channels:

- Reports can also be delivered directly via your point of contact at IMG or IMG's Director of Compliance on DPO@imgroup.co.uk or the HR Department on HR@imgroup.co.uk or;
- You can submit your concerns via the SPEAK UP REPORTING FORM.

Confirmation of receipt of the report to the Reporter can be expected within seven (7) working days and updates about its report status will be provided in accordance with applicable laws. Persons competent for the review of a report may reach out to the Reporter with follow-up questions and for clarifications.

Some concerns may be resolved by agreed action without the need for investigation.

4.2 Plausibility Check and Main Investigations

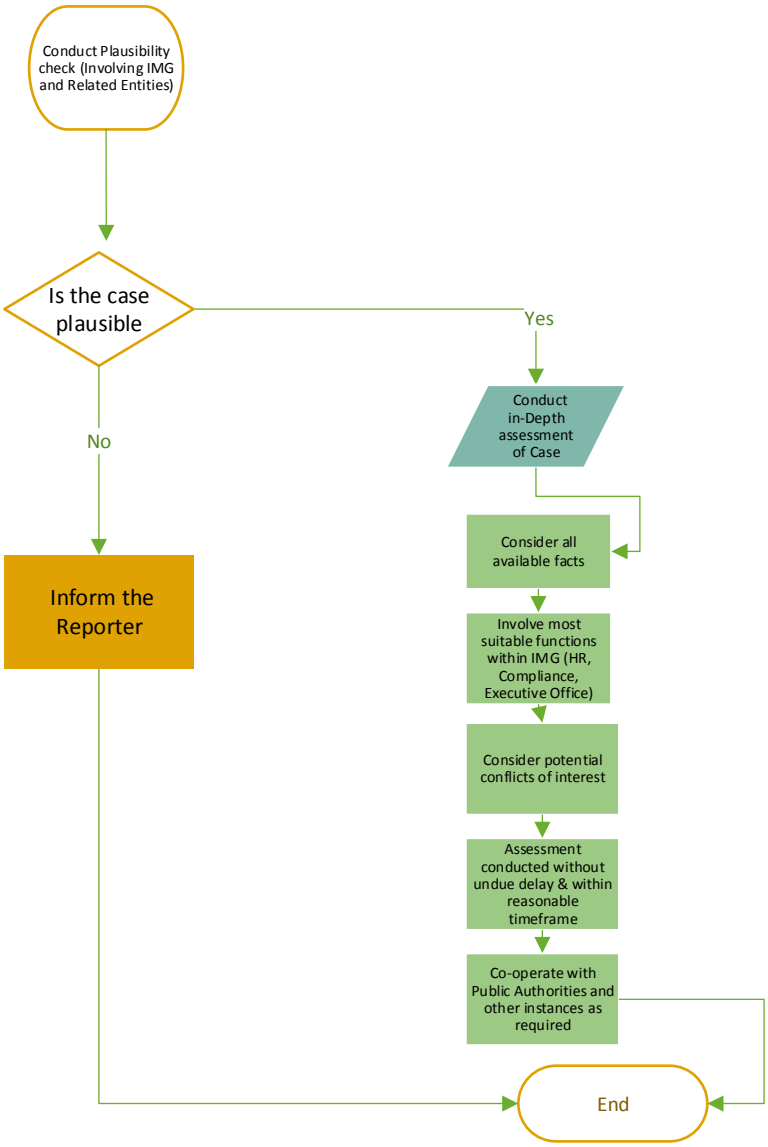
Through an initial **plausibility check** under the involvement of IMG and its related entities competent functions, implausible cases will be eliminated and closed. The Reporter will be informed accordingly.

Cases found plausible will be subject to main investigations. Such in-depth assessment of the case will consider all available facts and is undertaken under involvement of the most suitable functions within IMG (e.g., HR Department, Compliance, or Executive Office), in accordance with the nature of the case. Potential conflicts of interest (e.g., of the accused or the investigating parties) are duly considered.

The assessment of the facts is undertaken without undue delay and within reasonable timeframe considering the factual circumstances of the case (e.g., severity, complexity, information provided and evidence etc.). External resources for the assessment may be involved on a case-by-case basis as required. IMG will involve and co-operate with public authorities and other instances (data protection officer etc.) to the extent required under and in compliance with applicable laws.

As a result of the investigation, cases will be categorised and handled as follows:

- Reports on violations which cannot be proved will be closed as **unsubstantiated cases**. The closing decision is documented.
- Proven violations are rated as substantiated cases. These cases will be addressed with appropriate **remediation measures**.



4.3 Remediation measures

IMG will decide on a case-by-case basis how to appropriately address substantiated cases in the most effective way, considering inter-alia the following criteria:

- **Severity of the violation**: Assessment of degree of impairment (intensity or depth of an injury), and of number of people affected.
- **Probability of the violation**: Probability that a risk will materialise in a violation.
- **Urgency**: Pending risk or existing violation.
- **Category of the violation**: Categorisation of cases (e.g., criminal cases or offences) and circumstances (negligence, intent).
- **Reversibility of the violation**: Weighting of possibility of eliminating negative effects and required resources.
- **Area of violation**: IMG's own business area or violations by a supplier. Potential remedial measures inter-alia include:
    - Business partner notifications, warnings, request for certifications or audits.
    - Exercise of commercial leverage to stop a violation.
    - Measures to factually reverse or compensate remains of a violation.

Underlying remediation plans will be established by the concerned departments and are subject to approval by the Director of Compliance.

Remedial measures will be executed under supervision of competent IMG functions as foreseen in the remediation plan.

4.4 Closure and documentation

After successful application of remediation measures and subject to confirmation by the Director of Compliance cases will be closed. The decisions of closing cases will be documented. In addition, the relevant IMG functions (that may include HR, IT or Executive Office) will be informed about the closure of cases in order to derive the necessity for the adaptation or the adoption of new preventive measures.

4.5 Effectiveness Review

The effectiveness of this Policy and of remediation measures will be reviewed under the supervision of Director of Compliance on a regular basis and *ad hoc* as required. The Director of Compliance will provide IMG management with summary information on the status of proceedings under this Policy on a regular basis.

Review

This Policy shall be reviewed bi-annually. The next review date is March 2027.