# IMC GROUP

## Whistle Blowing Policy

# TABLE OF CONTENTS

# 1. THE WHISTLE BLOWING POLICY

## 1.1 Purpose & Scope

IMC Group (the 'Group') is committed to fostering a culture of corporate compliance, ethical behaviour and good corporate governance.

The Group's **Whistle Blowing Policy** ('Whistle Blowing Policy') is available to support and protect employees ('Employees') who may have concerns or queries about specific ethical issues or to report potential ethical breach or violations. The Whistle Blowing Policy applies to all Employees, individually and collectively, within the Group – this will be extended to third parties working with the Group over time as appropriate.

The purpose of the Whistle Blowing Policy is to encourage Employees who raise any concerns without the fear of reprisal or intimidation. The Group is committed to ensuring that whistleblowers will not suffer detriment for reporting potential **unacceptable conduct** ('collectively for ease of reference, hereafter referred as 'Unacceptable Conduct') in good faith, where the reporting procedure has been followed.

Any breach of law or any violation of the Group's Values or any other legal or ethical concern is referred to in this document as Unacceptable Conduct. For the avoidance of doubt, a potential breach or potential violation is not a breach or violation until such time as the matter is fully investigated and the allegation is substantiated in accordance with this Policy.

## 1.2 Unacceptable Conduct

Unacceptable Conduct covered by the Whistle Blowing Policy includes conduct that:

- is dishonest, fraudulent or corrupt
- is illegal, such as theft, drug sale or use, violence, harassment or intimidation, criminal damage to property or other breaches of prevailing laws and regulations
- is unethical or in breach of the Group's policies
- is potentially damaging to the Group, Employees or a third party such as unsafe work practices, environmental damage, health risks or substantial wasting of Group's resources
- may cause financial loss to the Group or damage its reputation or be otherwise detrimental to the Group's interests
- involves bribery or a conflict of interest
- involves harassment, discrimination, victimisation or bullying

# 2. REPORTING POSSIBLE ETHICAL ISSUES & VIOLATIONS

## 2.1 Ethical Filters for Decision Making

There may be occasions where we may be uncertain about the appropriate course of action. Ethical dilemmas may not always present themselves as 'right vs. wrong' – in some occasions, the problem may be seen as 'right vs. right.' In such situations, we need to ask ourselves if our decisions and actions are compatible with our Values.

Some questions can help us identify situations that may be unethical, inappropriate or illegal. These act as 'ethical filters' to aid us in our decision making. If you think the answer to any of the following questions may be 'No' or 'Not Sure', you should pause and may choose to discuss the situation further with your manager or the P&O department, where you feel appropriate. There will be strict security and protection around the confidentiality of your identity.

1. **Policies**
   Is it consistent with IMC's policies, procedures and guidelines?

2. **Legally Compliant**
   Is it legal?

3. **IMC Values**
   Is it aligned to our Values? Does it benefit the Group in the long term?

4. **Self**
   Can I share it openly without feeling uncomfortable?

## 2.2 Protecting Your Anonymity

The Group does not tolerate any retaliation against Employees who raise ethical questions or file a report ('Report') on questionable conduct/behaviour that may be in violation of the Group policies and guidelines.

To protect the anonymity of Employees, the following has been put in place:

1. The Group has engaged **In Touch**, a renowned international provider of compliance systems, to administer the Whistle Blowing Policy. In Touch serves more than 50 clients worldwide.

2. Report distribution of reported cases under the Whistle Blowing Policy is designed so that implicated parties are not notified or granted access to reports ('**Report**') they have been named in, even if they have been designated as report recipients for the particular category of violation. This ensures a complete and absolute protection of confidentiality and anonymity.

3. The third party reporting platform by In Touch does not generate or maintain any internal connection logs with IP addresses. No information linking your personal computer to the Whistle Blowing Policy is available.

You may refer to **Appendix 1** for the complete list of Frequently Asked Questions (FAQs) should you require more clarity on The Whistle Blowing Policy.

## 2.3 How to Raise an Ethical Concern

If you are aware of any possible, threatened or actual unethical conduct, including any violations of laws, regulations or any Group policies, you should report this promptly and consistent with the local laws of your country.

You can report an issue or seek advice on a matter in your local language through several confidential avenues provided by the Group-appointed vendor – In Touch. In Touch has been appointed as an independent third party vendor in order to provide a secure, anonymous and professional platform for you.

In Touch's platforms supports languages commonly used within the Group – *English, Chinese, Bahasa, and Thai.*

You can make a Report using any of the following resources which are managed by In Touch:

- Website: www.intouchwebsite.com/thecode
- Email: thecode@getintouch.com
- Toll free helpline which is available 24 hours a day, 365 days a year
    - Singapore: 800-101-2207
    - China: 10-800-713-1252
    - Indonesia: 001-803-015-204-7831
    - Thailand: 001-800-13-203-1937
- Voice Messaging System which is available 24 hours a day, 365 days a year

Should you have any doubt, a useful point of reference is that you need not first be absolutely sure that any of the relevant Group policies have been violated, before seeking assistance. The Whistle Blowing Policy is available to offer you guidance and address the issues you bring to our attention.

While your manager or P&O Business Partner may be able to assist you on violations reported, there is also good reason to use the reporting channels indicated above. The Whistle Blowing Policy ensures that your Report is promptly and securely addressed. More importantly, Reports may be filed anonymously and all Report information will be secure and held in the strictest confidence.

## 2.4 Following Up on a Report

The Group believes strongly in doing business and conducting ourselves in an ethical manner. Should a Report be submitted via the In Touch platform, it will be distributed to the appropriate Committee for investigation.

Separately, you may log into the In Touch website about three working days after reporting the violation to check if the Group has had any follow-up questions or requests.

The Whistle Blowing Policy Investigation Committee, without violating the confidentiality and the sensitivities of the case where possible, will provide you with an update when the violation has been investigated and conclusions drawn.

No retaliatory action will be taken or permitted against an Employee who reports potential unethical or illegal behavior in good faith (provided that person is not responsible for the breach).

## 2.5 False Or Unethical Reports

The Whistle Blowing Policy was initiated by the management of the Group on good faith and with the sole commitment of inculcating a culture of good governance and high ethical behaviour. As such, it is assumed that all reports are made with similar purpose and with no malicious intent to hurt or cause grievance to others. The Group will not tolerate false and irresponsible reporting, and where it is established that an Employee is not acting in good faith, and / or that he or she has knowingly made a false report. This will be regarded as a serious disciplinary matter and will be dealt with in accordance with the Group's disciplinary procedures.

Whilst not intending to discourage employees from reporting matters of genuine concern, Employees must exercise due care and diligence when making reports to provide complete details and relevant information that they have access to, which should exclude unsubstantiated rumors and hear-say.

## 2.6 Violation Categories

The following are some possible violation categories that we may use to guide us in reporting potential unethical behavior or practices within the Group. This list is meant as a guide and is not exhaustive in covering all possible violation categories that you may encounter. When in doubt, it may be appropriate to raise a Report so that Group management can investigate the issue in its entirety.

| Issue Type | Issue Descriptions |
|---|---|
| Accounting and Auditing Matters | The unethical systematic recording and analysis of the business and financial transactions associated with generally accepted accounting practices *(Examples include: misstatement of revenues, misstatement of expenses, misstatement of assets, misapplications of GAAP principles, wrongful transactions).* |
| Improper Disclosure of Financial Records | Careless, unlawful, intentional concealment or fraudulent conduct in recording, preparing, reporting, disclosing of either the value or the content of a contract, report, statement, document, record, or electronic file. |
| Embezzlement | To appropriate *(as property entrusted to one's care)* fraudulently to one's own use *(Examples include: misapplication of funds and mishandling of cash).* |
| Falsification of Contracts, Reports or Records | Falsification of records consists of altering, fabricating, falsifying or forging all or any part of a document, contract or record for the purpose of gaining an advantage or misrepresenting the value of the document, contract or record. |
| Unauthorized/Fraudulent Use of Group Facilities and Equipment | The misuse/abuse of Group services, equipment/software or assets. *(Examples include: destruction of an employer's property, visit of pornographic websites).* |

| Issue Type | Issue Descriptions |
|---|---|
| Improper Supplier or Contractor Activity | Supplier or contractor activity in violation of corporate policies and procedures; improper supplier or contractor selection based on personal gain, improper negotiation or diversion of contract awards. |
| Improper Receiving of Gifts | The receiving or solicitation of items which could be reasonably interpreted as an effort to influence a business relationship or decision; items received or solicited for the benefit of an individual or an individual's family or friends; items received or solicited during or in connection with contract negotiations; the acceptance of cash, checks, money orders, vouchers, gift certificates, loans, stocks or stock options. |
| Conflict of Interest | A conflict of interest is defined as a situation in which an employee, or a representative of the Group, has a private or personal interest sufficient to appear to influence the objective exercise of his or her official duties *(Examples include: inappropriate vendor relations, bribery, misuse of confidential information, inappropriate customer relations).* |
| Discrimination or Harassment | Uninvited and unwelcome verbal or physical conduct directed at an employee because of his or her sex, religion, ethnicity, or beliefs *(Examples include: bias in hiring, bias in assignments, wrongful termination, bias in promotions/training decisions, unfair compensation, inappropriate language).* |
| Employee Misconduct | Involves any employee conduct that is in violation of the Group's policies, employee handbook or any other printed materials that constitute employee conduct, and/or implied contractual responsibilities. Time abuse concerns about an employee who is falsifying his/her work hours. |
| Cheating / Theft | The act of cheating/stealing; specifically: the felonious taking and removing of personal property with intent to deprive the rightful owner of it. |
| Substance Abuse | Substance abuse is defined as the misuse of both legal and illegal drugs including alcohol *(Examples include: cocaine, narcotics, marijuana, stimulants).* |
| Abuse of or Fraud with Group Benefits | Improper, misleading or deceptive actions taken, falsification of records, or misrepresentation of physical conditions related to benefits plans including health and insurance plans, benefits reimbursement and sick or other paid time off programs. |
| Threat or Inappropriate Supervisor Directive | Improper use of supervisory authority; inappropriate management practices. |
| Disclosure of Confidential Information | Unauthorized and unlawful disclosure of corporately owned intellectual property or trade secrets, as well as employee, customer or consumer information, marketing and other corporate data bases, marketing plans, business proposals and strategies. |

| Issue Type | Issue Descriptions |
|---|---|
| Misleading Sales, Marketing & Advertisement | False, misleading or deceptive advertising, packaging, point of purchase displays or promotional materials; deliberately misleading messages, omissions of important facts or false claims about the Group's or competitors' products. |
| Copyright Violations or Software Piracy | Unauthorized use of corporately owned copyrights or software; also includes the use of unauthorized software on corporately owned systems. |
| Data Protection | Unauthorized access to and disclosure of personally identifiable personal data of employees and customers and other third parties that the Group possesses. |
| Environmental and Safety Matters | Failure to meet the requirements of any applicable law, rule or regulation relating to the environment, working conditions or workplace safety, including, without limitation, regulations promulgated by the local government. |

## 2.7 Violation Risk Levels

Reports will be activated to recipients based on the risk level of violation:

| Risk Level | Guidelines<br>*(each case may be assessed based on the appropriate context)* | Report Recipients |
|---|---|---|
| **High** | ▪ Has Group-wide implications<br>▪ Typically involving substantial sums of money for example and not limited to bribery, money-laundering & fund misappropriation | Group Level:<br>▪ Chairman<br>▪ Group Audit & Risk Governance Committee (GARGC)<br>▪ Group Board<br>▪ Group Internal Audit<br>▪ Group P&O<br>▪ Group CCO<br>Country Level:<br>▪ Country Head<br>▪ Country P&O |
| **Medium** | ▪ Usually Country or Location-specific<br>▪ Likely not involving money and even if so, is not of material sum – this is to be qualified by the respective stakeholders appointed in the preliminary assessment | Group Level:<br>▪ Chairman<br>▪ GARGC<br>▪ Group Board<br>▪ Group Internal Audit<br>▪ Group P&O<br>▪ Group CCO<br>Country Level:<br>▪ Country Head<br>▪ Country P&O |

*Reports categorized as 'N/A' may include invalid Reports (i.e. spam messages) or irrelevant content not relating to the Group.*

# 3. INVESTIGATION PROCESS

## 3.1 Investigation Process

The Group takes every Report submitted seriously. A complete and detailed investigation will be carried out. Upon receiving a Report, the Whistle Blowing Policy Process Owner will determine the appropriate stakeholders to conduct a preliminary assessment within 2 weeks of Report receipt, in consideration of the materiality & relevance of the Report.

An Investigation Committee (IC) will be convened within 7 working days of the Stakeholder Assessment, with an Investigation Officer (IO) to be nominated by the Investigation Committee. The IC is responsible for the full investigation of the violation and will provide periodic updates to Group Management.

The following details the investigation process on Reports that may be received from employees / initiated by the Group.

**Step 1** : **If a Report is initiated by an anonymous person through the In Touch website or Helpline:**

- The Group acknowledges receipt of the Report through the respective reporting avenue within 7 working days

**If a Report is received outside the formal channel or initiated by the Group:**

- The Group updates the Case into In Touch website within 7 working days

**Step 2:** The Whistle Blowing Policy Process Owner (elaborated on page 8) determines the appropriate stakeholders to conduct a preliminary assessment of the Report within 14 working days, in consideration of the materiality and relevance of Report

**If the Report warrants further investigation:**

- An Investigation Committee (IC) will be convened (within 7 working days of the preliminary Stakeholders' Assessment)
- The IC will lead the investigation. Updates will be provided by the Investigation Committee to the following based on violation risk level:
  - High risk: Convened by GARGC, followed by Fortnight Update*
  - Medium risk: Convened by Respective ExCom, followed by Monthly Update*
- IMC Group Chairman &/or GARGC Chairman may determine the investigation approach or reporting at his/their sole discretion.

**If the Report does not warrant further investigation:**
The Group responds to the Reporter (via In Touch) for formal closure of the Report

**Step 3** : Once investigations on the Report have been completed, a final update will be provided by the IC detailing:

- Full findings of the case
- Corrective actions recommended, if any
- Recommended change/s to existing processes / procedures to ensure that violations will not be repeated, if any

*(At the end of each quarter, a summary of all cases reported will be presented at the GARGC / Group Board where relevant. Cases received will be circulated monthly to GARGC Chairman including a short brief on rationale for each disposition and response provided. Reports can be provided at request by authorised recipients.)*

## 3.2 Whistle Blowing Policy Process Owners

For governance and controls purpose, the respective roles of the Whistle Blowing Policy Process Owner and Administrator are detailed below.

**Whistle Blowing Policy Platform Process Owner & Administrator – Report Recipients**

A. Head, Group Chief Corporate Officer (Process Owner)
B. Head, Group Internal Audit (Process Administrator)

**Report Exceptions**

*In the event of Reports directed at Recipient A:*

- Report to be routed (by In Touch) to GARGC Chairman

*In the event of Reports directed at Recipient B:*

- Report to be routed (by In Touch) to Head, Group Chief Corporate Officer

# APPENDIX 1: FREQUENTLY ASKED QUESTIONS (FAQS)

1. *What is the IMC Group Whistle Blowing Policy?*
2. *Who is In Touch?*
3. *Why do we need a Whistle Blowing Policy in IMC?*
4. *How can I submit a Report?*
5. *Does Management really want me to report?*
6. *Why should I report what I know? What's in it for me?*
7. *What type of situations should I report?*
8. *If I see a violation, shouldn't I just report it to my manager, security, or human resources and let them deal with it?*
9. *It is my understanding that any report I send from a Group computer generates a server log that shows every website that my PC connects with, and won't this log identify me as a report originator?*
10. *Can I file a Report from home and still remain anonymous?*
11. *I am concerned that the information I provide will ultimately reveal my identity. How can you assure me that will not happen?*
12. *Isn't this system just an example of someone watching over me?*
13. *I am aware of some individuals involved with unethical conduct, but it doesn't affect me. Why should I bother reporting it?*
14. *I am not sure what I have observed or heard is a violation of Group policy, or involved unethical conduct, but it just does not look right to me. What should I do?*
15. *Where do these Reports go? Who can access them?*
16. *What if my boss or other managers are involved in a violation? Won't they get the Report and start a cover-up?*
17. *What if I remember something important about the incident after I filed the Report? Or what if the Group has further questions for me concerning my Report?*
18. *Are these follow-ups on Reports as secure as the first one?*
19. *What if I want to be identified with my Report?*
20. *Can I still file a Report if I do not have access to the Internet?*
21. *Is the telephone toll-free reporting line confidential and anonymous too?*
22. *Who else can I contact if I have any further questions on the IMC Group Whistle Blowing Policy?*

1. **What is the IMC Group Whistle Blowing Policy?**

   The Whistle Blowing Policy provides a comprehensive and confidential reporting system managed by a third-party vendor, In Touch, for management and Employees to work together to ensure that the Whistle Blowing Policy and other working policies and guidelines of the Group are complied with.

2. **Who is In Touch?**

   In Touch is a third-party vendor which we have engaged to administer the Whistle Blowing Policy. In Touch is a leader among global ethics hotline providers. It was founded in 1991 and serves multinationals, private companies, public agencies and universities around the world.

   You may find out more about In Touch through their website: http://getintouch.com/

3. **Why do we need a Whistle Blowing Policy in IMC?**

   The Whistle Blowing Policy provides the platform from which a secure and independent channel is available to ensure that the Group as a whole continues to operate in a sustainable and ethical manner.

4. **How can I submit a Report?**

   You may submit a Report using various methods. The Whistle Blowing Policy provides several channels through which Employees may file a Report anonymously.

   The following table illustrates the options.

| The In Touch Website | Email In Touch | Toll-Free Call Centre |
|---|---|---|
| Click on the link to be provided by In Touch and you will be connected to the Whistle Blowing Policy landing page, hosted on In Touch's secure servers. | Send an email to the In Touch mailbox. This mailbox is managed by In Touch and they will inform IMC accordingly on your Report. | Refer to the International Toll-Free numbers and dialing instructions via the Whistle Blowing Policy. Leave a message in your local language. |

5. **Does Management really want me to report?**

   We certainly do. In fact, we need you to report. All of us, in our respective roles and relationships with our colleagues know and understand best what is going on in the Group - both good and bad. In certain instances, you may have initial knowledge of an activity that may be cause for concern.

   Your reporting can minimize the potential negative impact and implications on the Group. Providing positive input and proactive feedback will also help identify issues that can improve the strength of our corporate governance.

6. **Why should I report what I know? What's in it for me?**

   We all have the right to work in a positive environment. That expectation also brings with it the responsibility of acting ethically and doing the right thing - should we come across anything of concern

in the Group. It is through collaboration and a commitment to joint responsibility that we can strengthen the culture and how we work in the Group.

**7. What type of situations should I report?**

The Whistle Blowing Policy provides an avenue for sharing information for the Group's attention. You can file a Report of a violation or simply post an inquiry or suggestion. Please refer to the "Violation Categories" section of this document for the list of violation issues.

**8. If I see a violation, shouldn't I just report it to my manager or P&O and let them deal with it?**

You certainly can, but there are several good reasons why you should use the In Touch reporting platform as well.

Firstly, the In Touch platform ensures that your Report gets to the appropriate people. That may or may not happen if you simply report something to your manager, especially when dealing with issues not under his/her control. More importantly, Reports can be filed anonymously and all report information is secure and held in the strictest confidence.

**9. It is my understanding that any Report I send from a Group computer generates a server log that shows every website that my PC connects with, and won't this log identify me as a report originator?**

The In Touch platform does not generate or maintain any internal connection logs with IP addresses, so no information linking your PC to the Whistle Blowing Policy is available.

With fewer than 12% of Reports generated during business hours, most people prefer to report from the comfort of their home after hours and on the weekend.

**10. Can I file a Report from home and still remain anonymous?**

A Report from home, a neighbor's computer, or any Internet portal will remain secure and anonymous. An Internet portal never identifies a visitor by screen name and In Touch strips away Internet addresses so that anonymity is totally maintained. Plus, In Touch is contractually committed not to pursue a reporter's identity.

**11. I am concerned that the information I provide will ultimately reveal my identity. How can you assure me that will not happen?**

The reporting system is designed to protect your anonymity. However, you as a reporting party need to ensure that the body of the Report does not reveal your identity by accident, for example, "*From my cubicle next to John Doe…*" or "*In my 33 years…*"

**12. Isn't this system just an example of someone watching over me?**

The Whistle Blowing Policy concentrates on being a positive aspect of our overall corporate philosophy, and allows you to assure a safe, secure, and ethical workplace. You are encouraged to seek guidance

on ethical dilemmas, provide positive suggestions, or communicate a concern. Effective communication is critical in today's workplace and this is a great tool to enhance that communication.

We have carefully chosen the best reporting tool to meet our compliance obligations while maintaining a positive reporting environment.

**13. I am aware of some individuals involved with unethical conduct, but it doesn't affect me. Why should I bother reporting it?**

As an ethical enterprise, we choose to promote ethical behavior. All unethical conduct, at any level, ultimately hurts the Group and all Employees, including you. We only have to consider what happened in recent corporate scandals to see disastrous effects that a seemingly harmless lapse in ethics can have on an otherwise healthy company. If you do know of any incidents of misconduct or ethical violations, consider it your duty to yourself and your colleagues to report it.

**14. I am not sure what I have observed or heard is a violation of Group policy, or involved unethical conduct, but it just does not look right to me. What should I do?**

File a Report. The In Touch Platform can help you prepare and file your Report so it can be properly understood. We will rather you report a situation that turns out to be harmless than let possible unethical behavior go unchecked because you were not sure.

**15. Where do these Reports go? Who can access them?**

Reports are entered directly on the In Touch's secure servers to prevent any possible breach in security. In Touch makes these Reports available only to specific individuals within the Group who are granted the rights to evaluate the type of violation and location of the incident.

**16. What if my boss or other managers are involved in a violation? Won't they get the Report and start a cover-up?**

The Report distribution is designed so that implicated parties are not notified or granted access to Reports they have been named in, even if they have been designated as Report recipients for the particular category of violation.

In this case, the Report will be escalated and provided to the next higher level Report recipients.

**17. What if I remember something important about the incident after I filed the Report? Or what if the Group has further questions for me concerning my Report?**

When you file a Report on the web site or through the In Touch Call Center, you receive a unique user name and a password. You can return to the reporting system again either by Internet or telephone and access the original Report to answer questions posed by a Group representative and add further information that will help resolve open issues.

We strongly suggest that you return to the site in the time specified to answer the questions. This allows you and the Group to enter into an "anonymous dialogue" where situations are not only identified, but can be resolved, no matter how complex.

**18. Are these follow-ups on Reports as secure as the first one?**

All correspondences are held in the same strict confidence as the initial Report, continuing under the umbrella of anonymity.

**19. What if I want to be identified with my Report?**

There is a section in the Report for identifying yourself, if you wish to do so.

**20. Can I still file a Report if I do not have access to the Internet?**

You can file a Report from any computer that can access the Internet. You can file from home. Many public locations, including the public library or internet cafes, have computers with internet access. If you do not have access or are uncomfortable using a computer, you can call your In Touch toll-free reporting line which is available 24 hours a day, 365 days a year.

**21. Is the telephone toll-free reporting line confidential and anonymous too?**

Yes. You will be asked to provide the same information that you would provide in an internet-based Report and an interviewer will type your responses into the In Touch reporting platform. These Reports have the same security and confidentiality measures applied to them during delivery.

**22. Who else can I contact if I have any further questions on the IMC Group Whistle Blowing Policy?**

You may log onto the In Touch reporting platform and pose any further questions which you may have on the Whistle Blowing Policy.