

FRAUD & CORRUPTION PREVENTION POLICY

1. Overview

GPT is committed to creating and maintaining a culture of corporate compliance and ethical behaviour in which employees are responsible and accountable, behave with honesty and integrity and are able to raise concerns regarding unethical, unlawful or undesirable conduct, without fear of reprisal.

This policy seeks to comply with ISO 37001 – *Anti-bribery management systems – Requirements with guidance for use* and Australian Standard AS 8001 - 2008 *Fraud and corruption control*.

2. Purpose

Fraud and/or corruption, including bribery, in all forms are behaviours that are contrary to GPT's values and culture. GPT is actively committed to preventing fraud and corrupt conduct throughout the organisation. GPT has developed this fraud and corruption prevention policy as part of its overall risk management framework.

3. Scope

This policy applies to all GPT employees, contractors and Directors in relation to their GPT employment.

4. Definitions

Fraud and corruption includes the misappropriation of assets, the manipulation of reporting and the abuse of position for personal gain.

For the purposes of this policy:

- Fraud is a dishonest and intentional activity committed to secure an unfair or unlawful gain, regardless of whether or not deception is used.
- Corruption is a dishonest and intentional activity in which an individual acts against the interests of GPT and abuses their position of trust in order to achieve personal gain for themselves, another person or entity.

Examples include:

- Bribes, secret commissions or other improper payments or benefits
- The deliberate falsification, concealment, destruction or use of falsified documentation;
- The improper use of information or position;
- Theft of cash;
- Accounting fraud (for example, false invoicing);
- Giving or taking bribes or secret commissions or improperly accepting gifts;
- Using GPT intellectual property, information or resources (including computers) for personal gain;
- Theft or misuse of GPT assets, equipment or facilities;
- Use of GPT corporate credit card for personal expenses;
- Not disclosing conflicts of interest; or
- Improper conduct in procurement and/or contract management processes.

5. Policy

5.1 Reporting Fraud or Corruption

Individuals who become aware of potential fraudulent and/or corrupt behaviours should report these inappropriate behaviours as soon as possible to their manager and/or through existing internal issue resolution and reporting channels including People and Performance, Health and Safety incident reporting and the Chief Risk Officer (CRO). Where a manager receives a report they must inform the CRO.

If an employee does not feel able to use the existing reporting channels due to the nature and/or seriousness of the inappropriate behaviour, then they may raise the matter directly with the Whistleblower Officer:

- Email TheWhistleblowerOfficer@gpt.com.au
- Telephone (02) 8239 3926

GPT promotes a culture that expects and encourages the reporting of improper conduct including fraud and corruption and is committed to protecting people who disclose reasonably suspected mismanagement, corruption, illegality, or some other wrongdoing occurring at GPT. Refer also to the [Whistleblower policy](#).

5.2 Prevention of Fraud and Corruption

GPT will not tolerate dishonest, fraudulent or corrupt behaviour and is committed to preventing this behaviour, and encouraging an ethical culture in general, in the performance of its business operations.

As part of the GPT risk management framework and related governance processes GPT has established initiatives focused on the prevention, detection, investigation and reporting of suspected fraud against GPT. These initiatives include internal audits, fraud and corruption awareness training, risk assessments, robust internal controls, appointment screenings and management report reviews.

5.3 Investigation and management of reports of Fraud and Corruption

The CRO will determine the most appropriate approach for the investigation process. Employees and Managers must not initiate their own investigation.

All reports of suspected fraudulent activity will be dealt with having regard to applicable laws such as privacy, confidentiality, legal professional privilege and any requirements of natural justice.

Investigations into suspected fraudulent activity will be undertaken on the assumption of the innocence of the person implicated. All reports of improper conduct will be thoroughly investigated with the objective of locating evidence that either substantiates or refutes the claims made.

The rules of natural justice are to be observed in any investigation arising out of a report. The investigation will be conducted without bias and the person against whom the allegation is made should be given the right to respond.

Where it is found that an employee has knowingly or recklessly made a false report of fraud or corruption that conduct itself will be considered a serious matter and render the person concerned subject to disciplinary proceedings as provided by the Code of Conduct.

5.4 Consequences of committing Fraud or Corruption

Incidents of fraud and corruption, including bribery, are viewed very seriously by GPT.

GPT will decide whether or not to bring civil proceedings, refer for criminal prosecution or take disciplinary action, or a combination of these actions. Where appropriate, GPT will vigorously pursue the recovery of money or property lost through fraud or corruption.

5.5 Roles and responsibilities

Sustainability and Risk Committee

The Sustainability and Risk Committee is responsible for ensuring there is an appropriate approach to fraud and corruption prevention in place and for receiving regular reviews of the fraud and corruption prevention policy.

Chief Risk Officer (CRO)

The CRO is responsible for establishing a fraud and corruption prevention framework including:

- Regular review and communication of this fraud and corruption prevention policy;
- Development and maintenance of a fraud and corruption prevention plan; and
- Maintenance of appropriate insurance protection arrangements.

The CRO is also responsible for co-ordinating investigations into allegations of fraud and corruption with assistance from the Internal Audit and People and Performance teams where required and in consultation with senior management where appropriate.

Managers

Managers are responsible for ensuring that employees in their team are aware of and comply with:

- This policy and related policies and procedures; and
- GPT internal controls and limits of authority.

Employees

Employees are responsible for:

- Complying with this policy, related policies and GPT internal controls including limits of authority;

- Raising concerns regarding improper conduct or inappropriate behaviour with their manager or through other reporting channels made available by GPT, including the Whistleblower Officer; and
- Co-operating with any investigations related to suspected breaches of this policy.

6. Further information

GPT's expectations in relation to the reporting of improper conduct and inappropriate behaviour included in the new employee induction program and as part of ongoing training and awareness programs.

If you require additional information about this policy and/or you have any questions issues or concerns, please contact the CRO.

7. Related policies, procedures and guidelines

- Acceptable Use Policy (Technology)
- Anti-Money Laundering and Counter-Terrorism Financing Policy
- Code of Conduct
- Conflicts Management Policy
- Limits of Authority
- Personal Dealing Policy
- Procurement and Expense Management Policy
- Recruitment guidelines
- Travel and Entertainment Policy
- Supplier Code of Conduct
- Whistleblower Policy