Financial Crime Policy:

Anti-Fraud, Bribery & Corruption, and Tax Evasion and Financial Crime Sanctions

1. Introduction

This policy sets out the general rules and principles in relation to fraud, bribery, corruption and the facilitation of tax evasion and financial sanctions (together, "**Financial Crime**") to which Great Portland Estates plc and all its subsidiaries ("**GPE**") adhere.

It is GPE's policy to conduct all our business in a legal, honest and ethical manner. We should always be mindful of our Values 'We achieve more together', 'We are committed to excellence' and 'We are open and fair'. We are committed to the prevention of Financial Crime, and we will not tolerate fraud, bribery or any form of corrupt practice, nor the evasion of tax or breach of financial sanctions. All employees of GPE, as well as third parties working with and for us, are expected to share this commitment and familiarise themselves with the types of improprieties that could occur in their areas of responsibility and be alert to any indications of Financial Crime.

The purpose of this policy is to (i) set out our responsibilities, and those working with and for us, in observing and upholding our position on Financial Crime; and (ii) to provide an overall framework to equip those working for us on how to recognise and respond to any instances of Financial Crime.

If you are in any doubt as to what is required or expected of you in relation to this policy, please contact your line manager, or alternatively the General Counsel & Company Secretary or Deputy General Counsel.

2. Who does this policy apply to?

This policy applies to everyone who works for GPE and its joint ventures. All employees and those working for us are required to read and comply with this policy.

This policy will be communicated to those working for us at the outset of our business relationship with them and as appropriate subsequently.

3. Why is this policy important?

Bribery, corruption and fraud are criminal offences which are punishable for individuals by up to ten years' imprisonment and, if GPE (or its employees or those working for us) is found to have taken part in Financial Crime, it could also face criminal liabilities and an unlimited fine. Charges may also be brought against the directors and officers of a company if that company commits a bribery or fraud offence and they consented or connived in such an offence.

This policy is also important to protect GPE's good reputation that has been fostered over many years. GPE's ability to tender for new business and our relationship with customers, suppliers, contractors, joint venture partners, local authorities and agents depends a great deal upon the good reputation that we have established which could be diminished by any form of dishonesty or Financial Crime.

As a Group we therefore take our responsibilities very seriously.

An employee who commits Financial Crime will face disciplinary action and may face civil action and/or criminal prosecution. GPE may terminate its contractual relationship with any third party who does not comply with the principles of this policy.

4. Definitions

4.1. *What is Fraud?*

Fraud can broadly be defined as the deliberate use of deception or dishonesty to make a gain/ advantage or to cause a loss to or to economically or financially (usually financial) disadvantage another person or party.

The core fraud offences in the UK are set out in the Fraud Act 2006 which creates a general offence of fraud with three possible ways of committing it:

- **Fraud by false representation** – is when someone dishonestly makes a false representation, knows that the representation is (or might be) untrue or misleading, and does so with the intention of making a gain for themselves or another, or to cause a loss to another, or expose another to a risk of loss;
- **Fraud by failing to disclose** – is when someone dishonestly fails to disclose to another person information which they are under a legal duty to disclose and in doing so intends to make a gain for themselves or another, or to cause a loss to another or expose another to a risk of loss; and
- **Fraud by abuse of position –** is when someone occupies a position in which they are expected to safeguard, or not act against, the financial interests of another person, and they dishonestly abuse that position, and intend, by means of the abuse of that position, to make a gain for themselves or another, or to cause a loss to another or expose another to a risk of loss.

In any of the scenarios above, no gain or loss needs to actually occur, only the intention to make a gain or cause a loss is required.

The Company may be held criminally liable for fraud offences where one of its senior managers committed an offence acting within the actual or apparent course of their duties. Two or more people agreeing to commit fraudulent activity would also be guilty of the common law offence of 'Conspiracy to Defraud'. The table below sets out some examples of actions that would be considered to be fraud.

Examples of Fraud

- Knowingly generating or paying false claims or invoices;
- Forgery and/or tampering with any corporate documents, records or accounts;
- Misappropriation or use of company assets for personal gain;
- Wilful destruction or removal of company records;
- Falsification of travel and subsistence claims;
- Inflating property valuations;
- Deliberate misapplication of accounting policies.

4.2. What is Bribery?

Bribery is promising, offering, giving, requesting, or accepting any "advantage" to induce or reward behaviour that is illegal, unethical or a breach of duty, including the misuse of office or power for private gain or to obtain a business advantage.

Bribery does not have to involve cash or an actual payment exchanging hands or anything tangible. It can take many forms such as a gift, lavish treatment during a business trip, tickets to an event or other favours, such as offers of employment or free services.

The Bribery Act 2010 creates four prime offences:

- offering, promising, or giving a bribe;

- requesting, accepting, or agreeing to receive or accept a bribe;

- bribing a foreign public official (the definition of a foreign public official is broad and essentially includes anyone performing a public role, as well as those working in state-owned enterprises); and

- failure of a corporate entity to prevent an associated person (i.e., being an employee, agent, consultant, or anyone else performing services on behalf of GPE) from bribing on its behalf. (There is a defence to this offence where the organisation can show it had adequate procedures in place to prevent bribery.)

If the offence is proved to have been committed with the consent or connivance of a senior officer of the organisation, then the senior officer may be personally liable.

The Company may be also liable for the offence of bribery if one of its senior managers participated, in the actual course of their duties, in the act of bribing, or being bribed.

These offences cover public and private sector bribery, those who offer/pay bribes and those who request/receive them, and bribery committed directly or through third parties.

See sections 5 and 6 below for specific behaviours that would also be treated as an act of bribery.

Examples of Bribery

- You are offered an unusually generous gift or offered lavish hospitality by a third party or a third-party requests the same from you in return for a business advantage e.g. to win a planning appeal or a contract;
- An employee or contractor acting for us makes an improper payment to a government official in connection with a planning, building inspection or other matter;
- A supplier offers to provide services to you personally at below market rates in exchange for you using your influence to secure them a contract;
- An agent acting on our behalf makes a payment or gift to an official to speed up an administrative process or in return for another advantage (see section 5 below);
- Attempting to cover up an employee or business mistake by offering a gift.

4.3. *What is Tax Evasion?*

UK Tax evasion means the offence of cheating the public revenue or fraudulently evading UK tax. It occurs when a person knows they have an obligation to account for tax but dishonestly, either through an action or omission, does not do so.

Individuals, corporate bodies (such as companies) and partnerships evading tax may or may not try to take steps to disguise or misrepresent what they are doing. The key is that the individual, corporate body or partnership is aware that tax is due and deliberately does not pay it. It is possible to evade tax without involving others but in many cases, others will be involved.

Foreign tax evasion means evading tax in a foreign country, provided that the conduct is an offence in that country and would also be a criminal offence if committed in the UK. As with tax evasion, the element of fraud means there must be deliberate action, or omission with dishonest intent.

Tax evasion facilitation means being knowingly concerned in, or taking steps with a view to, the fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, or aiding, abetting, counselling or procuring the commission of that offence. Tax evasion facilitation is a criminal offence, where it is done deliberately and dishonestly.

Under the Criminal Finances Act 2017, a criminal offence is automatically committed if an "associated person" of GPE, being an employee, agent, consultant or anyone else performing services on behalf of GPE, deliberately and dishonesty takes action to facilitate UK or foreign tax evasion. GPE may be liable for failing to prevent that facilitation and may face criminal sanctions unless it can show that it had 'reasonable prevention procedures' in place.

The Company may additionally by liable for tax evasion through the acts of its senior managers.

It is important to note that tax evasion is not the same as tax 'avoidance'. Tax avoidance is where a person, often acting on professional advice, has entered into arrangements designed to legally minimise their tax liabilities.

The above are some practical examples of fraud, bribery, corruption and tax evasion. The lists are non-exhaustive and in case of doubt you should raise the matter with your line manager or the General Counsel & Company Secretary or Deputy General Counsel.

Examples of Tax Evasion

- A third-party deliberately fails to register for VAT;
- A third-party requests that payments be made under an invoice for goods or services that does not reflect the true purpose of the payment;
- A supplier seeks to evade tax by asking to be paid into an offshore account to deliberately and dishonestly hide their income which you suspect will not be declared in the UK for UK tax purposes;
- An employee asks to be paid as a contractor in order to reduce their tax liability.

Who can commit Fraud, Bribery or Facilitation of Tax Evasion?

Financial Crime can be committed by anyone; this includes employees, workers, consultants, third parties who perform services for us or on our behalf, or anyone that has a relationship with GPE such as a supplier, agent, contractor or customer. It is therefore crucial to remain vigilant and look out for signs of improper activity.

5. Facilitation Payments and kickbacks

Facilitation payments are typically small unofficial payments paid to public officials to secure or speed up an administrative process or government action by an official. This could include officials of any government department or agency (such as any council officials and planning officers), political parties, executives and employees of government owned/run companies and anyone holding a legislative, administrative or judicial position. Kickbacks are typically payments made in return for a business favour or advantage and GPE does not make or accept kickbacks of any kind.

Facilitation payments are treated as bribes under the Bribery Act and you must not pay or accept facilitation payments of any kind to or from a government official. The exception is where it is legitimate to pay for an application to be 'fast tracked' and this service is an official service offered to the general public at the official fee.

If you are requested to make a payment on GPE's behalf, you must ensure that payments requested are proportionate to the goods and services provided and you should always request a receipt which details the reason for the payment.

Additional caution must be exercised before offering hospitality (or any other benefit) to a public official. You must ensure you comply with GPE's Gifts & Hospitality Policy and also confirm with the official that they would not be breaching their own relevant codes of practice.

In case of doubt, you should raise the matter with the General Counsel & Company Secretary.

6. Donations

GPE will not make donations to political parties.

We are committed to delivering GPE's Social Impact Strategy and supporting worthy causes in the communities in which we work. Charitable donations in GPE's name may be permitted, provided they are made properly, transparently and not for the personal or financial benefit of a customer, supplier or other third party or their families with whom GPE has a business relationship. Such charitable donations must not improperly influence the recipient or be in exchange for any business advantage and must be approved in advance by the Social Impact Committee.

7. What are Financial Crime Sanctions?

Financial sanctions are restrictions imposed by the United Kingdom on dealing in specific areas of trade or offering certain services with respect to a specific country (e.g. Russia), and/or directly or indirectly providing funds or economic resources to designated individuals or companies within or related to that jurisdiction or within a specific high-risk sector.

The Sanctions and Anti-Money Laundering Act 2018 governs the UK sanctions regime, and is supported by numerous country-specific regulations, such as the Russian (Sanctions) (EU Exit) Regulations 2019. At the date of this policy, sanctions are currently in place in respect of over 20 separate countries worldwide and numerous designated terrorist organisations.

Separate sanctions regimes are imposed by both supra-national organisations, and independent states, including the United Nations, the European Union, the USA, Australia and Canada.

Those subjected to financial sanctions in the UK will include those who are identified ("designated") on lists published by the Office of Financial Sanctions Implementation (OFSI), as well as any companies owned or controlled by, or individuals acting at the behest of designated individuals. Therefore it is not always immediately apparent whether a counterparty is the subject of financial sanctions.

GPE addresses its financial sanctions risk by screening all counterparties (i.e. all parties to transactions in its property investment business and all customers in its property leasing business) before entering into transactions with those parties. This screening is provided via a third party service provider which is currently, 'SmartSearch'. GPE also requires screening of all potential new suppliers prior to their engagement. Again, via SmartSearch.

SmartSearches screening is conducted via GPE's Group Financial Controller. Any results that raise a potential sanctions issue will be reviewed by GPE's Money Laundering Reporting Officer ("MLRO") and his approval must be sought prior to proceeding with any transaction or engagement. The Group Financial Controller will review any updates/alerts received from SmartSearch as and when they arise and discuss them with the MLRO if necessary.

In the event of a potential sanctions match, the MLRO may take legal advice from professional advisers as appropriate.

Examples of UK Financial Sanctions Breaches

- Selling land to a sanctions designated buyer using overseas shell companies where true ownership cannot be identified nor appropriate due diligence be conducted.
- Receiving monies from a third party on behalf of a sanctioned person or entity.
- Providing a lease to a commercial or residential customer who is a designated person.
- Engaging and making payments to a supplier for goods or services who is a designated person or from a country to which restrictions are applied.

Who can commit financial sanctions breaches

Breaches of UK Sanctions Regulations could result in the commission of a criminal offence, which is punishable by financial penalties, and/or a prison sentence.

The offences can be committed by individuals and, if breaches are committed in the course of GPE business, the Company could also be investigated and prosecuted alongside any individual and face an unlimited fine. In addition, breaching financial sanctions can result in serious reputational damage, exclusion from financial markets and restrictions on business activities. It is crucial that we all comply with financial sanctions to avoid these legal and financial repercussions.

8. Responsibilities

8.1. Board/Audit Committee

The Board has overall responsibility for general oversight of this policy including:

- establishing a culture to encourage ethical behaviour and compliance with this policy by employees;
- monitoring the effectiveness and implementation of this policy through the Audit Committee which shall review this policy (and other appropriate associated policies) annually;
- receiving reports on compliance with this policy through the Audit Committee; and
- ensuring appropriate mechanisms are established for reporting Financial Crime.

The Chief Executive has specific responsibility for the implementation of this policy and managing the overall risk of Financial Crime.

8.2. General Counsel & Company Secretary

The General Counsel & Company Secretary, in conjunction with the Director of Investor Relations & Financial Reporting and (in respect of aspects concerning the facilitation of tax evasion) the Director of Corporate Finance, will assist all employees by reviewing, refreshing and reinforcing this policy and guidance on a regular basis.

8.3. Directors of/Heads of Department

Directors of and Heads of Department are responsible for:

- overseeing and ensuring compliance with this policy by individuals within their departments;
- ensuring all employees within their departments complete required Financial Crime training;
- identifying and assessing Financial Crime risks in their respective areas and maintaining effective procedures and controls within their departments to mitigate those risks;

- monitoring any suspicious activity within their departments or involving third parties; and promptly reporting suspicious activity, as set out in section 9 below.

8.4. Employees

It is the responsibility of every GPE employee (including employees of joint ventures) to report, prevent, detect and manage Financial Crime risks on a day-to-day basis. This includes but is not limited to:

- ensuring that you read, understand and comply with this policy;
- avoiding any activity that might lead to, or suggest a breach of this policy;
- ensuring that internal controls and processes are continuously complied with and that relevant systems and controls continue to operate effectively;
- acting with propriety in the use of GPE's resources and not allowing company property or assets to be misused or misappropriated;
- ensuring that you complete all required training and development in relation to Financial Crime;
- ensuring that appropriate due diligence processes are followed when engaging third parties;
- co-operating fully with any internal or external checks, reviews or investigations; and
- raising any concerns or suspected irregularities as soon as possible.

9. Record Keeping

We must keep financial records and have appropriate controls in place to evidence the business reason for making and receiving payments to or from third parties and to prevent improper payments. All payments must be authorised in accordance with GPE's procedures and all accounts, invoices and other records relating to dealings with third parties must be prepared and maintained with accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

All employees must disclose and register gifts and hospitality in accordance with GPE's Gifts & Hospitality Policy and ensure that expense claims relating to gifts and hospitality are submitted in accordance with the GPE Expense Claims and Petty Cash Expenses Policy.

10. Detection and Reporting

It is your duty to report all suspected Financial Crime as soon as practicable. Appendix 1 sets out a non-exhaustive list of practical examples or "red flags" which may indicate improper activity in relation to Financial Crime matters.

If you suspect or become aware that a Financial Crime or irregularity has occurred, you must raise your concerns as soon as possible with the General Counsel & Company Secretary or in accordance with GPE's Whistleblowing Policy, which includes the option to report the matter via Safe Call, our independent and confidential reporting facility (telephone: 0203 117 2520 or email: whistle@pcaw.co.uk).

If you are unsure whether a matter should be reported, you should initially speak with your line manager or, if you feel unable to do so, with the General Counsel & Company Secretary, or alternatively, Safe Call. It is better to voice your concerns than stay silent and allow potential wrongdoing to go unchecked or not be investigated properly.

Any information that you may provide will be dealt with in the strictest confidence and the safeguards set out in GPE's Whistleblowing Policy will apply to you. It is GPE's policy that whistleblowers will not suffer any detrimental treatment as a result of raising a concern in good faith.

Speed is of the essence and such initial report can be verbal but must be followed up within 24 hours by a written report which should include all known details and bases for the concern, which may include the following (so far as known):

- the amount/value of any Financial Crime, if established;
- the position regarding recovery (if appropriate);
- the period over which the wrongdoing or irregularity occurred, if known;
- the date of discovery and how the suspected wrongdoing or irregularity was discovered;
- whether the person(s) responsible or involved has/have been identified;
- whether any collusion with others is suspected;
- what evidence of the wrongdoing is available;
- details of any actions taken to date; and
- any other information or comments which might be relevant.

On discovery of a potential concern, it is essential that you do not take any action that could prejudice an investigation or criminal proceedings. You must not contact anyone suspected to be involved in the irregularity in order to establish further facts or resolution and you must not discuss the matter with any person save as set out in this policy or the Whistleblowing Policy.

11. Investigation

A preliminary review will be conducted to validate the suspicion raised and assess whether the case is substantiated enough to start an investigation.

Investigations will be performed in accordance with the established procedure defined in the Whistleblowing Policy and in accordance with GPE's Financial Crime Investigation Guidelines.

Upon completion of the investigation GPE will determine the course of actions to be taken, including application of any required legal and disciplinary measures, in all cases where deemed appropriate.

If any significant instances of Financial Crime are identified, management may consult external third-party specialists on the appropriate course of action and case management protocols in the given circumstances. This may result in information being passed on to the police, Serious Fraud Office or other governmental or law enforcement authorities for further investigation.

12. Training and Awareness

An important aspect of this policy and its effectiveness is the general awareness and responsiveness of employees throughout GPE. Training on this policy forms part of the induction process for all new joiners. Employees will also receive periodic refresher training, particularly those in more relevant roles.

All employees are made aware of this policy (and other relevant policies) via various channels of communication, including via the GPE intranet.

In addition, to provide a deterrent to employees and to prevent future recurrence of any Financial Crime that is discovered, a brief and anonymised summary of an incident may be published and distributed within the Group to share information and lessons learned.

Third parties and associated persons should ensure that staff are appropriately trained to understand, prevent and report Financial Crime.

13. Monitoring and review

All employees must be aware of Financial Crime risks and take appropriate action if you detect or suspect Financial Crime.

The identification of the key Financial Crime risks facing GPE and the implementation of appropriate management and control procedures are key to our detecting and preventing Financial Crime. A Financial Crime risk and controls assessment will be carried out at least every two years or more regularly if necessitated by changes to the business or external events.

Compliance with this policy will be reviewed and reported to the Audit Committee on an annual basis. Employee compliance will be monitored through activity reporting and the annual employee attestation process. Assurance regarding internal control systems and procedures will be sought through the delivery of internal audits or other assurance reviews. Our external auditor also provides independent assurance on financial matters relevant to their responsibilities.

14. Conclusion

We are all responsible for ensuring that GPE remains free from improper practices. This policy provides an overview of the relevant Financial Crime offences and many of the steps GPE takes to mitigate its risks. This policy is supported by a number of other GPE policies, as set out below, which should be read in conjunction with this policy. You are responsible for ensuring that you read, understand, and comply with these policies and procedures:

- Ethics Policy;
- Whistleblowing Policy;
- Anti-Money Laundering and Counter-Terrorist Financing Policy;
- Gifts & Hospitality Policy;
- Expense Claims and Petty Cash Expenses Policy;
- Inside Information and Share Dealing Policy;
- Use of the Group's Suppliers Policy and Involvement with Third Parties (disclosure of potential conflicts) Policy; and
- IT Policy (IT security requirements).

If you have any questions about this or any of the associated policies above, please address them in the first instance to your line manager. If they cannot be answered by your line manager, please contact the General Counsel & Company Secretary or Deputy General Counsel.

This policy may be amended from time to time.

Appendix 1 – Potential Risk Scenarios: Fraud, Bribery, Corruption, Facilitation of Tax Evasion and Financial Sanctions "Red Flags"

This is a list of possible red flags that may arise during the course of your day to day work for GPE and which may raise concerns under various laws and regulations relating to Financial Crime. This list is not intended to be exhaustive and is for illustrative purposes only.

Please note that if you encounter any suspected or actual Financial Crime, you must report it as soon as practicable as set out in section 9 above:

Fraud

a) A supplier is submitting false invoices for goods and or services that are not being provided;

b) You notice unnecessary or inappropriate purchases being made through third parties;

c) You notice an increase in the number of invoices being generated by one department;

d) An employee's lifestyle changes with no obvious explanation as to why. For example, expensive cars, jewellery, clothes;

e) Missing documents, or only photocopied documents are available when an original is required;

f) Discrepancies between paperwork and verbal explanations;

g) Pressure or other incentives are applied by management on the external valuers in order to misstate the property valuation, whether to support the value to be recorded in the financial statements or for another purpose;

h) Cash balances are deliberately overstated e.g. through fraudulent disclosure of overnight deposits;

i) GPE internal controls are not properly enforced or are overridden;

j) An employee reports inconsistent, vague or implausible responses arising from enquiries;

k) An employee is resistant to others taking over or seeing their work, for example avoids taking time off; or

l) A third party contacts GPE claiming to be a supplier and seeks to change the bank account details held for that supplier in order to intercept payment.

Bribery & Corruption

a) A third party insists on receiving a commission or fee payment before committing to sign up to a contract with GPE or carrying out a government function or process for GPE;

b) A third party demands or requests lavish entertainment or gifts before commencing or continuing contractual negotiations;

c) You are offered an unusually generous gift or offered lavish hospitality by a third party;

d) A third party insists on the use of side letters or refuses to put terms agreed in writing;

e) A third party refuses to agree terms that require compliance with anti-bribery laws;

f) You receive an invoice from a third party that appears to be non-standard or customised;

g) A third party requests that a payment is made to "overlook" potential legal violations;

h) You notice that we have been invoiced for a commission payment that appears large given the service stated to have been provided;

i) You become aware that a third party engages in, or has been accused of engaging in, improper or questionable business practices;

j) A third party requests or requires the use of an agent, intermediary, consultant or distributor or supplier that is not typically used or known to GPE;

k) A supplier requests that you provide an employment opportunity or another advantage to a friend or relative; or

l) An employee or a third party is offered or receives a backhander for appointing a certain third party to deliver services or goods.

m) An employee managing a tender process accepts backhanders for selecting certain suppliers;

Tax Evasion or the Facilitation of Tax Evasion

a) A third party requests payment in cash and/or refuses to sign a contract or fee agreement or to provide an invoice or receipt of payment;

b) A third party insists on payments being made to an entity that is different to that which GPE has a contractual relationship with;

c) A GPE customer or supplier has an uncommon, overly complex ownership structure without a reasonable explanation for the complexities;

d) A third party suggests GPE participates in a transaction that appears to be circular or has no commercial rationale;

e) A supplier indicates that they have not disclosed income or assets to tax authorities or have otherwise not complied with their tax obligations;

f) A supplier fails to raise any appropriate invoices for their work or services;

g) A supplier requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

h) A supplier insists on payments to be made/received to/from a bank account held in a different name without a justifiable reason;

i) GPE is made aware that a customer or supplier has previously made a disclosure to HMRC under the disclosure of tax avoidance scheme (DOTAS) regime or an overseas equivalent;

j) A supplier indicates an unwillingness to accept GPE's terms and conditions with respect to the facilitation of tax evasion; or

k) A supplier offers a discount in return for their invoices to be settled in cash.

Financial Sanctions

a) Selling land to a buyer using overseas shell companies where true ownership cannot be identified nor appropriate due diligence be conducted.

b) There is no obvious commercial reason for a transaction or its terms.

c) The counterparty changes their name by deed poll without a reasonable explanation.

d) Due diligence cannot be performed and the counterparty is resistant to it.

e) A counterparty has undertaken a complex restructuring without a clear business rationale.

f) Use of corporate vehicles to obscure true ownership, sources of funds and/or the jurisdictions involved, including the use of shell companies.

g) Involvement of third parties (e.g. for providing payments) which could hide involvement of designated persons.