# IP Group plc and its Group of companies

# Failure to Prevent Fraud Policy & Procedures

IP Group plc ("**IP Group**" or the "**Group**") operates a zero-tolerance approach to fraud and is committed to the prevention, deterrence and detection of fraud. This document sets out the Group's policy against fraud (the "**Policy**") and the standards and procedures required to ensure compliance with it.

The Group does not tolerate any form of fraud within its business, and we expect our officers, employees, subsidiaries and other persons who act for or on our behalf to act with honesty and integrity and to conduct themselves in accordance with this Policy, and compliance with this Policy is mandatory for all these persons.

We will not tolerate any of our officers, employees, agents or business partners committing or knowingly assisting or encouraging fraud to benefit (directly or indirectly) the Group.

We are committed to the following principles:

- We will carry out business fairly, honestly and openly.
- We will not provide services or sell goods where we know or suspect that they will or may be misused by a customer for fraudulent purposes anywhere in the world.
- We will not buy services or goods from any supplier where we know or suspect them of acting fraudulently or not to be properly declaring their income and/or any relevant tax or duties in connection with those activities.
- Our clear policy is not to engage in transactions where fraudulent activity is present or suspected to be present, even if it may result in the Group losing business.
- We expect our agents and others who represent us to also commit to these principles.

Any employee or other person found to be in breach of these principles will face disciplinary action; however, no employee will suffer demotion, penalty, or other adverse consequence for refusing to engage in transactions where tax evasion or fraud is suspected. Please see 'Consequences of Non-Compliance' below for further details.

We also operate a strict policy and procedures to ensure that we do not assist our customers, suppliers, other business partners, employees or contractors to engage in aggressive tax avoidance or other fraudulent activity. If we have any doubts, we will refer the issue to the Chief Financial & Operating Officer.

This Policy applies irrespective of the country in which business is being conducted. Where there are differences between the requirements of local law and the provisions of this Policy, you must comply with whichever sets the highest standard of behaviour.

Although this Policy is non-contractual and we may make changes to it from time to time, we expect everyone to always comply with the principles in this Policy and people will be held accountable for their behaviour in relation to this Policy.

## Policy Objective

The purpose of this Policy is to set out expectations and responsibilities for the Group and for those working on our behalf, in observing and upholding our zero-tolerance of fraud in our business. Specifically, this Policy contains information and guidance on how to recognise and avoid becoming victims of fraud or violating any applicable fraud laws. Notably, applicable fraud laws include the offence of failure to prevent fraud (the "**FTPF Offence**"), created by sections 199-206 of the UK's Economic Crime and Corporate Transparency Act 2023 ("**ECCTA**").

## Why is this Policy important?

For individuals working for or on our behalf, fraud (including tax evasion), is a criminal offence in most countries in which we operate, and the penalties can be severe. In many countries the penalty includes a custodial sentence or fines.

As a result of the FTPF Offence, the Group may be also held criminally liable where a fraud offence (which is an offence under UK law) is committed by an officer, employee, subsidiary or any other associated person (as defined in section 1 of this Policy below), for our benefit unless we are able to demonstrate that we have reasonable fraud prevention procedures in place.

If convicted of the FTPF Offence, the Group may be liable for an unlimited fine and may also suffer major reputational damage and potentially loss of business as a result. Having a criminal record may also bar the Group from operating in certain sectors or doing certain kinds of work or mean that other businesses will not work with the Group anymore. The overall effect for the Group would potentially be very damaging to the strength or viability of our business. We wish to ensure that the Group does what it can to avoid this and to guard itself against deliberate breaches of economic crime laws including, but not limited to, fraud.

Please note that there is a defence to the FTPF Offence where the Group can demonstrate that it had 'reasonable procedures' in place to prevent fraud at the time the FTPF Offence was committed. The Group's 'reasonable procedures' include, but are not limited to, this Policy and ensuring compliance with, and enforcement of, the principles and procedures contained within it.

## What is expected of you?

All **Staff** (as defined in section 1 on page 3 below) must read and observe the requirements of this Policy. Staff must also act with honesty and integrity and comply with all applicable laws, whether or not specifically covered by this Policy or any of our other policies.

**Managers** should work to create an environment that encourages compliance with this Policy. Supervision of responsible business practices is as important as supervision of performance.

**Business Partners and Contracting Partners** (as defined in section 1 on page 3 below) are expected to adhere to this Policy. Business Partners and Contracting Partners must also act with honesty and integrity and comply with all applicable laws, whether or not specifically covered by this Policy or any of our other policies.

This Policy cannot address every conceivable situation. In many circumstances, the law or this Policy will clearly dictate what you should do, but on other occasions the situation will require you to exercise judgement.

Any concerns relating to a breach of this Policy should be reported to the Chief Financial & Operating Officer.

**Date of publication: 9 September 2025**

# Failure to Prevent Fraud Policy & Procedures

## 1. Introduction

This Policy applies to our directors, officers and employees (referred to as **"Staff"**). We expect the highest standards from our Staff and will not tolerate anyone engaging in fraudulent activity or helping another person to do so.

We will also endeavour to ensure that people and businesses who perform services for us or on our behalf, for example, agents, advisers, consultants and contractors (referred to as **"Business Partners"**) act in accordance with the underlying principles set out in this Policy whilst performing those services.

We also expect all companies or entities with whom we enter into a collaboration, partnership, joint venture, consortium or similar relationship (referred to as **"Contracting Partners"**) to comply with the Policy.

Staff, Business Partners and Contracting Partners are referred to collectively in this Policy as "Associated Persons".

## 2. What is Fraud?

**Fraud is a criminal act which typically involves the intentional deception of another person for personal or financial gain or to cause loss to another.**

The term ‘fraud’ commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering or extortion. Fraud can reduce company profits, damage the Group’s culture and its reputation.

Examples of potential fraud at IP Group may include, but is not limited to, the following:

a) fraud by false representation (where a person makes a representation which they know to be untrue or misleading);
b) fraud by failing to disclose information where there is a legal duty to do so;
c) fraud by abuse of position;
d) false statements by Staff to deceive shareholders or creditors;
e) destroying, altering or forging company documents;
f) obtaining services dishonestly;
g) causing a loss to the Group or another party (such as a member of Staff, Business Partners, Contracting Partners or suppliers);
h) false accounting/misleading underlying records;
i) knowingly creating or paying false claims or invoices;
j) carrying out business for any fraudulent purpose; and
k) tax evasion.

Individuals, such as those working for or on behalf of the Group, will typically be liable for their own fraudulent acts.

In some jurisdictions, legal persons may also be held liable for the actions of others and, in the case of the FTPF Offence, their Associated Persons (see definition above). Under the FTPF Offence, the Group may be held criminally liable where a specified fraud offence (which is an offence under UK law) is committed by an Associated Person for its benefit, unless the Group is able to demonstrate that it has reasonable fraud prevention procedures in place.

The prevention, detection and reporting of fraud are the responsibility of all Associated Persons and, as with anti-facilitation of tax evasion, it is also important to bear in mind that the criminal law may treat a person as having knowledge if they 'turn a blind eye', particularly if there is an upside for them in doing so (i.e. treating them as aiding, abetting, counselling, or procuring the commission of fraud). If you suspect someone to be engaged in fraudulent activity, you must report your suspicions in line with the Group’s Reporting Procedures below.

**Tax Evasion**

Tax evasion is an important example of fraud which may affect the Group. Tax evasion is when a person knows they have an obligation to account for tax but dishonestly does not do so.

That person may try to take steps to disguise or misrepresent what they are doing in order to conceal the liability, but this is not essential.

Tax evasion needs to be contrasted with what is sometimes known as tax 'avoidance'. Avoidance is where a person, usually acting on professional advice, has entered into arrangements designed to minimise their tax liabilities. In many

cases, the tax authorities accept that the arrangements are effective, but in some cases they may challenge the structure and may be successful in showing that tax is actually due. The attempt to avoid the tax liability is unsuccessful but provided the person had an honest belief that the planning was going to be effective, even if proven wrong, it does not amount to evasion.

In many cases, it is possible to evade taxes without involving another person. However, in some cases it is inevitable that other people may be involved.

For example, the evasion may involve trying to go undetected by misdescribing the services that have been rendered to the Group which generate the tax liability. This could involve misdescribing what the services were, the country in which they took place, or the person or entity which carried them out. If a member of Staff was to accept or not challenge the misdescription, that person may be 'facilitating' the tax evasion. If that person knew it was a misdescription, that would be criminal facilitation and that person is likely to be committing a criminal offence.

In these circumstances, the individual could be personally liable for the criminal offence of 'facilitating' the tax evasion. IP Group may also be liable under the Criminal Finances Act 2017, if the person facilitating the tax evasion is an Associated Person (as defined above), and this will be the case whether the tax evaded is owed in the UK or in a foreign country.

## 3. Risk of Fraud (incl. Tax Evasion) at IP Group

The Group has undertaken a detailed risk analysis of the key areas of the Group's business to assess the three elements of the fraud triangle:

i) **Opportunity**: Do Associated Persons have the opportunity to commit fraud and are there areas where there is higher opportunity, weak controls and/or inadequate oversight in place?
ii) **Motive**: Are there financial or operational stresses, needs to meet targets, culture to turn a blind eye or disincentivise speaking-up?
iii) **Rationalisation**: To what extent is there a prevalence of fraud within the business, resentment, failure to see any harm and/or failure of adverse consequences of speaking-up?

Key risk areas where fraudulent activity may be carried out which could benefit the Group or others were assessed and mapped as below:

| RISK AREA | FRAUD PREVENTION PROCEDURES | RESIDUAL RISK RATING |
|---|---|---|
| Customers | • Annual training for staff<br>• Skilled staff<br>• Contractual provisions<br>• Money Laundering Reporting Officer ("MRLO") sign off requirements<br>• Speaking-up hotline | LOW |
| Suppliers | • Annual training<br>• New supplier on-boarding process<br>• Skilled staff<br>• Appropriate payment controls in place<br>• No cash payments<br>• Contractual provisions<br>• Speaking-up hotline | LOW |
| Staff | • Annual training<br>• Skilled staff<br>• Robust expense review and approval processes<br>• Gifts and Hospitality reporting and monitoring<br>• Appropriate payment controls in place<br>• Conflicts of interest policy<br>• Contractual provisions<br>• HR onboarding checks | LOW |

| | | |
|---|---|---|
| | • Staff undertaking corporate finance mandates are approved by the relevant regulated entity Board and a full consideration of their training and competency, fitness and propriety is reviewed annually by the relevant regulated entity Compliance Officer<br>• Speaking-up hotline | |

## Staff

Staff are a key constituent for identifying and reducing the potential or actual instances of fraud across the business. Employees receive annual training on the prevention of fraud (including anti-facilitation of tax evasion) and are made aware of the Group's speaking-up hotline and associated reporting procedures. In addition, the Group ensures that adequate controls are in place, with regular reviews of its payment and board authorities. The annual and, where applicable, half-yearly accounts of IP Group plc and, where applicable, its core subsidiaries also undergo external audit or review (as applicable) to ensure the robustness of financial information and their underlying controls.

**Red flags** - Staff should look out for fraudulent activity "red flags". Any red flags should be reported immediately through the Reporting Procedures detailed in section 5 below. These red flags may include:

- Operation outside of the Group's payment and/or expenses policy;
- Bypassing of procedures/controls;
- Manipulation of financial data (e.g. false accounting, overstating valuations);
- False identity documentation;
- Obtaining of services dishonestly;
- Backdating of contracts;
- Misrepresentations and/or false statements in order to receive investment or lending into the Group and/or its portfolio; and/or
- Payments to new suppliers without appropriate new supplier checks (see below 'Customer and Suppliers' for further red flags).

We expect the same standards from our external Business Partners and Contracting Partners as we do from our Staff. Our business could be criminally liable if a Business Partner or Contracting Partner engages in fraudulent activity in connection with their relationship with us.

Business Partners and Contracting Partners must be carefully selected, subject to contractual controls and monitored. It is important that the Group only works with Business Partners and Contracting Partners who it is confident will not engage in fraudulent activity. Any agreement entered into with a Business Partner or Contracting Partner must contain fraud prevention contractual provisions, with all contracts being reviewed by a member of the Group's Legal Team prior to their finalisation.

### Customers

As identified in the Group's risk analysis, the Group's employee investment director roles on its portfolio companies may give rise to circumstances where Staff or an agent may act fraudulently for the benefit of the Group, either directly or indirectly. Such examples may include:

- Knowingly approving incorrect R&D tax credits;
- Seeking discounts from contractors in return for cash payments or which are known to be for concealing earnings from tax authorities; or
- Making false statements to deceive potential shareholders, purchasers or auditors.

The Group also carries out fund management services. As a fund manager there is a risk that the Group may facilitate tax evasion or fraud. Examples include:

- Accepting subscriptions from investors which are known or expected to be for the purposes of money laundering;
- Accepting proceeds for the sale of an investment where it is known or suspected to be for the purposes of tax evasion e.g. investments made via complex overseas structures where ultimate beneficial owners are obscured;
- Fund managers may be under additional pressure to raise funds in a difficult economic climate or be encouraged to accept investment funds if offered higher management fees;

- Carry schemes and performance fees available may encourage individuals to ignore third-party fraud or tax evasion; or
- Fraudulently altering documents or coaching a client on how to pass AML checks.

Should Staff suspect any of the above then these should be reported immediately through the Reporting Procedures detailed in section 5 below.

Suppliers

Suppliers at IP Group are mainly providers of professional services and regular office services and expenses. Suppliers are predominantly UK-based and payments are made via BACS by our experienced accounts payable team. All payments are approved in accordance with the payment authorities (including as to the number and identity of required approvers and their relevant authorisation limits) specified in the Group's Board Authorities which are reviewed and renewed annually by the Board.

The Group's procedures reserve the right to conduct additional due diligence checks, which may include some or all of the following:

- making it a condition of doing business with us that customers and suppliers will act diligently to correctly account for any taxes they may owe under the law;
- undertaking additional checks on their ownership structure or on where their business is managed so that we understand the country or countries in which they should be paying tax;
- asking them to prove they are registered for tax by asking for details of their tax registrations;
- when we buy goods, products or services, undertaking additional checks to ensure that tax has been paid on those goods as appropriate, in particular when the goods have been imported or are subject to internal excise taxes; and
- any other procedures which we consider to be reasonable in the circumstances to undertake.

**Red flags – customers/suppliers**

Any customer/supplier red flags should be reported immediately to the Chief Financial & Operating Officer. These red flags include:

- the customer or supplier refusing or failing to confirm that it will comply with the Group's additional due diligence checks;
- the customer or supplier operating or being resident in a market or country where there is a high risk of tax evasion;
- uncertainties existing about why the customer or supplier is buying our goods or services, or the price which they are prepared to pay;
- the customer or supplier having unusual invoicing or documentation practices;
- the customer or supplier refusing to give the Group or its Staff access to its books and records when this is reasonably requested and required by the Group; or
- the customer or supplier requesting for payments to be:
  - made in cash;
  - paid to or through another entity;
  - paid to bank accounts in countries other than the country where services are performed;
  - paid to offshore bank accounts;
  - paid in a currency other than the local currency; or
  - paid in advance of the services being performed.

### Informing Business Partners and Contracting Partners about this Policy

All Business Partners and Contracting Partners (whether individuals or companies) should be made aware of this policy. In addition, the Group may decide to provide fraud awareness or training to higher-risk Business Partners and Contracting Partners.

Before entering into a relationship with a Contracting Partner, thorough due diligence should be conducted on any prospective partner. A risk assessment should be conducted first to determine the appropriate level of due diligence. Staff should contact the Senior Compliance and Risk Manager for help with the form of risk assessment to use and the level of due diligence to conduct.

## 4. Bookkeeping and Accounting

**Books, records and accounts must be kept accurately and fairly reflect all transactions.**

Staff, Business Partners and Contracting Partners must not make, approve, or process any payment which relates to the Group's business with the intention, understanding or suspicion that any part of the payment is to be used for any

purpose other than that described by the documents supporting the payment. No "off the books" or unrecorded funds or accounts are permitted.

**Examples of prohibited record keeping activities include:**

- making records appearing to show a payment to one person when, in fact the payment was made to, or intended for, someone else;
- submitting inaccurate expenses;
- records that inaccurately characterise or inaccurately describe the true nature of transactions or payments
- claims for services, products or equipment not received; and/or
- creating or maintaining any unrecorded funds or assets of the company, including unrecorded "petty cash".

## 5. Reporting Suspected Non-Compliance

Any Staff member, Business Partner, Contracting Partner, customer or supplier must report any breaches or potential breaches of this Policy as soon as possible. You can report your concerns to your Manager, the Group General Counsel or the Chief Financial & Operating Officer, or in accordance with the steps outlined in our Speaking-Up Policy which can be found on our website at Governance and policies – IP Group plc.

IP Group will take all reported concerns seriously and will confidentially investigate to determine if the law or this Policy has been contravened.

## 6. Consequences of Non-Compliance

The Group will actively investigate all breaches or suspected breaches of this Policy.

IP Group may take appropriate disciplinary action, including termination of employment, against any member of Staff who fails to comply with this Policy or applicable laws. In addition, a member of Staff who breaks the law may be reported to the police and may face criminal proceedings, fines or imprisonment.

For Business Partners and Contracting Partners, non-compliance with this policy and any applicable laws will likely be a material breach of contract and may result in the termination of any relationship with the Group and the matter being reported to the police or other appropriate regulatory authorities.

## 7. Effective Monitoring

IP Group will establish and maintain an effective system for monitoring compliance with this Policy. A regular monitoring plan has been implemented to ensure that this is done, which will be submitted to the Audit & Risk Committee for approval.

The Chief Financial & Operating Officer is responsible for the day-to-day oversight of this policy.

## Who can I contact if I have any questions?

If you have any questions about anything in this Policy or about any related issue which is not covered in this Policy, please contact the Chief Financial & Operating Officer or the Group General Counsel.