croudacegroup

Anti-Fraud Policy

1. Introduction

This Policy sets out the standards that are expected by Croudace Homes Group Limited and its subsidiary companies ("the Group") of all its employees agents or consultants and any other person or body acting on its behalf. Further, the Group expects the same approach to doing business from suppliers and sub-contractors and any other third party dealing with the Group. When working for or with the Group, you are agreeing to and are obliged to ensure that you understand and comply with this policy.

Through its Directors, the Group takes steps to assess the risk to its business and the particular areas within it that may be particularly vulnerable to fraud. Appropriate training and procedures have been put in place on a targeted basis to prevent fraud. The anti-fraud policy will be reviewed in the light of changes in legislation or where events dictate (e.g. after any known attempted fraud) but in any event is the subject of periodic review at Group Board level.

Third parties working for or with the Group will be expected to provide additional information or clarification where requested to ensure that the Group is satisfied as to full compliance with its policies and procedures.

Compliance with this anti-fraud policy is mandatory.

2. Fraud

According to ActionFraud, the UK's national reporting centre for fraud and cybercrime, fraud can be simply described as occurring when 'trickery' is used to gain a dishonest advantage (often financial) over another person or business.

The offence of fraud is defined in the Fraud Act 2006 as either:

- dishonestly making a false representation with a view to gain or with intent to cause loss or expose to a risk of loss;
- dishonestly (and with a view to gain or with intent to cause loss, etc) failing to disclose information when under a legal duty to disclose it; or
- dishonest abuse of position, with a view to gain or to cause loss, etc. It is irrelevant whether gain, loss or exposure to loss actually occurs.

Fraud is a major issue affecting individuals and businesses in every country and in every sector. Fraud can be incredibly damaging. It can affect the Group in two ways, i.e. where the Group:

- is the intended victim of the fraud; and
- fails to prevent an "associated person" committing fraud intending to benefit

the Group, or in some cases, its customers.

For examples of potential fraudulent activities affecting the Group see Appendix 1.

3. Failure to prevent fraud

The Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023) introduced a corporate failure to prevent fraud offence, which captures a wide range of fraud offences committed for the benefit of the Group, including:-

- fraud by false representation;
- fraud by failing to disclose information;
- fraud by abuse of position;
- obtaining services dishonestly;
- participation in a fraudulent business;
- fraudulent trading; and
- cheating the public revenue.

There is only one relevant defence to the corporate offence of failure to prevent fraud: when the fraud offence was committed, which is that the Group had reasonable prevention procedures in place, or that it was not reasonable to have any such procedures in place (e.g. if the risk of fraud being committed was extremely low). The government has published detailed guidance on the failure to prevent fraud offence and reasonable prevention measures it expects organisations to adopt, and the Group has factored this guidance into this policy and related procedures. This policy is central to those prevention procedures.

The Group is committed to ensuring compliance with the ECCTA 2023. If the Group were convicted of this offence it could face unlimited criminal fines.

Risk assessments:

The Group has conducted an assessment of the nature and extent of the Group's exposure to the risk of employees, agents and other associated persons committing fraud and of the Group's exposure to the risk of falling victim to fraud.

While it is not possible to anticipate all potential fraud risks, the Group's fraud risk assessment covers various key pinch-points, e.g.:

- opportunity, e.g. weak controls and inadequate oversight;
- motive, e.g. financial stress and meeting targets; and
- rationalisation, e.g. no harm and resentment.

While there are some natural overlaps with the Group's risk assessments in other areas of crime prevention, this assessment is specifically tailored to and focussed on fraud risks.

The Group's procedures take account of the level of control and supervision the Group is able to exercise over its operations, particularly in relation to people acting on its behalf, including, for example, staff and contractors.

This risk assessment in relation to fraud is available to staff on request. You should read this risk assessment, especially the part applicable to the area of the business that you work in or for, to better understand areas of risk around fraud so that you can be vigilant. Also if you identify or think that there might be fraud risks which are not covered by that risk assessment then please let your relevant Director know. The fraud risk assessment is not intended to be static and will be reviewed and updated on a regular basis. The fraud risk assessment is not to be shared externally outside the Group.

Associated persons:

The definition of 'associated person' under ECCTA 2023 is wide. The Group has identified types of associated persons relevant to the Group as follows:

- staff;
- agents;
- contractors providing services for or on the Group's behalf; and
- sub-contractors.

Additional fraud prevention procedures:

The Group's risk assessment recognises that different associated persons may present different fraud risks and the need for implementing procedures that are proportionate to the identified risks and the size and nature of the business, including carrying out the following procedures:

- The Group undertake pre-employment vetting checks plus ongoing vetting checks for roles considered to present a higher risk of fraud;
- The Group keeps its reward and recognition systems, including commissions, bonuses, financial targets, etc, under regular review;
- The Group conducts due diligence on employees, contractors, and other associated persons to ensure they are trustworthy and understand their responsibilities;
- The Group manages fraud risks throughout all procurement processes with associated persons, i.e. pre-tender, tender, contract management, during project delivery and project extension;
- New and existing associated persons are subject to strict anti-fraud contractual terms, which are subject to review;
- The Group has robust fraud detection measures in place. Although the Group will naturally scrutinise larger transactions, the Group will apply an appropriate level of scrutiny to its smaller transactions and lower-risk operations as well; and
- The Group also collects and maintains information on potential conflicts of interest.

For Property specific fraud examples and fraud prevention procedures see Appendix 2.

4. Why is fraud prevention Important?

Criminals could target our Group:

- to enable them to commit a fraud;
- with the intention of illegally gaining access to our sensitive data or client account; and/or
- with the intention of becoming a colleague, otherwise known as an “infiltrator”.

Also fraud may occur when someone who would not normally be classed as a criminal sees an opportunity to gain from committing fraud.

The consequences of committing fraud cannot be overstated and may include any of the following:

- The individuals can be sentenced to long prison sentences for committing fraud;
- The Group can be prosecuted under ECCHA 2023 for failing to prevent fraud;
- The Group could be liable to pay significant financial penalties;
- The Group could face immeasurable reputational damage; and/or
- There could be significant losses for customers or suppliers.

Failing to comply with this policy, and related procedures, could weaken the Group’s fraud prevention framework and thereby leave the Group vulnerable to falling victim to fraud.

As such, the Group takes compliance with this policy and related procedures very seriously.

Because of the importance of this policy, failure to comply with any requirement of it may lead to disciplinary action under the Group’s procedures, and this action may result in dismissal for gross misconduct. Any non-employee who breaches this policy is liable to have their contract with the Group terminated with immediate effect.

5. Policy

The Group and the Group Board do not tolerate fraud and is committed to preventing, detecting and reporting fraud, and reducing its exposure to the lowest possible levels.

The Group aims to limit its potential exposure to any acts of fraud by implementing various fraud prevention procedures, including the following:

- The Group promotes employee awareness of its anti-fraud policy and procedures through targeted policies and training identified and reviewed by the Directors responsible for the respective departments. All staff within high-risk areas receive fraud-prevention training periodically so that they can recognise and avoid situations where there is the possibility of fraud, either by themselves or others;
- The Group has set a clear anti-fraud policy and reviews it and its procedures and its fraud risk assessment periodically at Director and Group Board level.
- The Group encourages staff to be vigilant and immediately report any suspicions of fraud or actual instances of fraud;
- The Group will rigorously investigate any instances of alleged or suspected fraudulent activity and will take any appropriate action (whether internal disciplinary action or external reporting to the relevant authorities) which may also lead to legal action and criminal sanctions. Please see section 8 for further details;
- The Group does not offer or agree to make improper or fraudulent payments to agents, contractors, public officials, or anyone that the Group does business with;
- The Group engages and remunerates agents, consultants and other third parties only for legitimate services and requires third parties to comply with appropriate due diligence checks to ensure appropriate transparency and minimise the chance of fraud. The Group may apply a higher level of due diligence to associated persons working in high risk areas;
- The Group seeks to ensure fraud threats are identified and risks mitigated through maintaining effective systems, controls and processes, including verifying the identity of all potential staff, customers and third parties (i.e. significant suppliers), risk assessing/monitoring entities and relationships, implementing security controls to minimise unauthorised access, sharing fraud risk intelligence across the Group and ensuring customers ad staff are provided with necessary information to help protect against fraud;
- The Group's internal accounting systems are designed (and externally audited on an annual basis) with suitable checks in place to prevent individuals being able to process illegitimate payments or create false records;
- This anti-fraud policy and its associated procedures do not operate in isolation; they form part of and should be read and followed alongside the Group's other crime prevention measures, including:
- Anti-bribery policy;
- Anti-bribery guidance note; and
- Whistleblowing policy.

6. Responsibility

While the Group Board plays a leadership role in relation to fraud prevention, particularly in relation to reviewing and signing off risk assessments, responsibility for the day-to-day operation of the anti-fraud policy and related procedures rests with the

Directors of the Croudace group companies. They have the full support of the Group Board, which will ensure direct access to our most senior people as they think necessary, even where their primary reporting lines differ.

Also managers have responsibility for preventing and identifying fraud and risks of fraud,

Fraud prevention is the responsibility of everyone associated with the Group, including staff, agents, contractors and other associated persons. The Group encourage colleagues and those it works with to challenge views that tend to support or seek to 'normalise' fraudulent behaviours.

7. Reporting concerns

Fraud is never acceptable. The Group encourages everyone to speak up early if they encounter fraudulent practices, or have any ethical concerns, no matter how minor. It is essential that everyone promptly raises any concerns in relation to possible fraudulent activity, of whatever nature. This also applies if you only suspect that fraudulent activity is being carried on or may be carried out. If you have any concerns you should report them.

The correct reporting mechanism will depend on the nature of the suspected activity, e.g.:

- where an individual is concerned that a member of staff or agent is committing or has committed fraud, a whistleblowing report may be appropriate. Please see the Group's Whistleblowing policy;
- where an individual is concerned that the Group has been the victim of fraud, please raise this with your immediate manager in the first instance.

You must make your report as soon as reasonably practicable and may be required to explain any delays. Concerns may be raised anonymously, if preferred.

To avoid the risk of committing a **"tipping off"** offence under section 333A or 342 of the Proceeds of Crime Act 2002 (POCA), no one else should be informed of your report without the approval of the Group Legal Director or Regional Company Solicitor.

You must report any actual or suspected fraud. Failing to report any fraud or suspicion of fraud is a disciplinary matter.

8. Responding to a fraud incident

Total protection from fraud is not possible. In the event that the Group falls victim to, or is used for fraudulent activity, the Group has procedures for responding to that fraud to manage the incident swiftly and effectively.

Central to the Group's response procedures is early detection, so prompt reporting of any concerns or suspicions is vital.

The Group will investigate all internal concerns raised appropriately and in a timely manner.

Where a fraud incident is confirmed, the specific actions the Group will take will depend on the nature of the fraud, but generally the Group may:

- consider whether to take any legal action, e.g. obtain an injunction or freeze assets;
- make necessary and appropriate notifications, e.g. to banks, insurers, customers, etc;
- Take disciplinary steps in relation to staff (which may lead to dismissal from employment) or in the case of third party contractors or agents then suspension or termination of their relevant contracts may be required;
- seek external expert advice; and/or
- consider whether it is necessary and appropriate to self-report to prosecution authorities such as the police.

The Group will then feed any fraud events into subsequent risk assessment activities.

Please note that these procedures are policy guidelines and the Company reserves the right to amend them from time to time. They are not contractual but are a term of your employment or engagement and with which you must comply

Appendix 1 – Fraud examples:

- **Scenario 1 (Group is a victim of fraud):** The Group hires a contractor to supply and install high-quality materials for a new development. The contractor agrees to the terms and provides a quote for the materials and labour. However, once the project begins, the contractor:
    - **Uses Substandard Materials**: Instead of the high-quality materials specified in the contract, the contractor uses cheaper, lower-quality materials to cut costs and increase their profit margin.
    - **Overbilling**: The contractor submits invoices for materials and labour that were never provided or performed, inflating the overall cost of the project.
    - **Double Billing**: The contractor bills the Group for materials that were already paid for or bills multiple clients for the same materials.
    - **Kickbacks**: The contractor receives kickbacks from suppliers for purchasing materials at inflated prices, which are then billed to the Group.

  Such fraudulent activities can lead to significant financial losses for the Group, delays in project completion, and potential legal issues if the substandard materials do not meet building codes or safety standards.

- **Scenario 2 (Group fails to prevent fraud):** A procurement manager of the Group is responsible for selecting suppliers and contractors for various projects. To benefit the Group, a member of staff engages in the following fraudulent activities:
    - **Bribery:** offers bribes to local government officials to expedite the approval of planning permissions and inspections. This allows the Group to start and complete projects more quickly, giving the Group a competitive advantage in the market.
    - **Kickbacks:** The procurement manager receives kickbacks from suppliers and subcontractors in exchange for awarding them contracts. These kickbacks may then be funnelled back into the Group's accounts or used to reduce project costs. For example, a supplier might inflate their invoice amounts and then secretly return a portion of the payment to the procurement manager or the Group.

  While these fraudulent activities could be viewed as leading to significant financial gains for the Group by reducing costs and speeding up project timelines, they expose the Group to significant legal risks, reputational damage, and potential penalties if the fraud is discovered. Fraud, even where it benefits the Group, is never tolerated.

Appendix 2 – Property fraud:

As a house builder, property fraud is a real concern to the Group. It takes many forms and can involve:

- fraudsters offering 'get rich quick' investments (e.g. property millionaire scams);
- attempts to acquire ownership of property using forged documents or impersonating the buyer; and/or
- property title/registration fraud.

Property fraud also covers involvement in the transfer of moneys by professionals or other individuals in the conveyancing/sale process.

Typical signs of property fraud include:

- the customer's conveyancer involved in the transaction has an email address from a large-scale web-based provider, e.g. Gmail, Yahoo Mail or Hotmail;
- the customer's conveyancer involved does not appear on the register of their professional body, e.g. the SRA's Solicitors Register or Council of Licensed Conveyancers' Find a CLC Lawyer;
- the deposit is not paid by the customer, but by a third party;
- there are plans for a sub-sale or back-to-back transactions on the property.

The presence of one or more of these factors does not automatically indicate fraud, but they are warning signs that the Group should investigate further. Individuals should pay particular attention to matters where a number of factors are present.

The Group seeks to protect its organisation from property fraud in various ways, including having robust customer due diligence processes, ensuring any identity documentation provided is properly scrutinised to ensure they appear authentic and show no apparent signs of being forged or altered.

The Group will routinely apply source of funds checks to property matters, especially where a high-risk factor is present, e.g.:

- the purchase of a property is being funded solely from the proceeds of a related sale and a new mortgage;
- substantial private funding is involved;
- third party funding is being used;
- funding arrangements are unusually complicated; or
- the matter involves corporate or overseas funding.

The Group does not accept cash as a form of payment.