ANTI-FRAUD POLICY

1 POLICY STATEMENT

1.1 It is the policy of Hargreaves Services plc and its subsidiaries (**Group**) to conduct all business in an honest and ethical manner.

1.2 We take a zero-tolerance approach to fraud and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate, implementing and enforcing effective systems to counter fraud.

1.3 We take our responsibilities very seriously. We will uphold all laws relevant to fraud in all the jurisdictions in which we operate. However, we remain bound by the laws of the UK, including the Economic Crime and Corporate Transparency Act 2023.

2 ABOUT THIS POLICY

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and of those working for us, in observing and upholding our position on fraud; and

(b) provide information and guidance to those working for us on how to recognise and deal with fraud issues.

3 WHO IS COVERED BY THE POLICY?

3.1 This policy applies to all individuals working at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located (collectively referred to as **workers** in this policy).

3.2 The subsidiaries covered by this policy include but are not limited to: Hargreaves Industrial Services Limited; Hargreaves (UK) Limited; Blackwell Earthmoving Limited; Hargreaves (UK) Services Limited; S&B Utilities Limited; C.A Blackwell (Contracts) Limited; Hargreaves Land Limited; Hargreaves Waste Management Services Limited; Hargreaves Industrial Services (HK) Limited; Hargreaves Power Services (HK) Limited; Access Services (HK) Limited; Hargreaves Services South Africa (Pty) Limited; and Hargreaves Industrial Services Sdn Bhd.

4 WHAT IS FRAUD?

4.1 The term ‘fraud’ commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, or extortion. For the purpose of this policy, fraud includes but is not limited to the following:

(a) fraud by false representation - where a person makes any representation as to fact or law, express or implied, 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) participating in a fraudulent business;

(e) obtaining services dishonestly;

(f) misappropriating property (including electricity, gas, and water);

(g) false accounting/misleading underlying records;

(h) false statements by company directors to deceive members or creditors;

(i) fraudulent trading, meaning to carry out business for any fraudulent purpose;

(j) cheating the public revenue; and

(k) presenting a misleading document.

5 WHAT IS NOT ACCEPTABLE?

5.1 It is not acceptable for you (or someone on your behalf) to:

(a) make any representation as to fact or law, express or implied, which you know to be untrue or misleading;

(b) manipulate information given to a customer of the Group or used by the Group to form judgements and formulate strategies;

(c) abuse your position of authority by act or omission in a way that is contrary to the financial interests of the Group or its customers or suppliers;

(d) disclose confidential information to anybody (including third parties and other workers) without having authority to do so;

(e) use your private and personal interests to influence their decisions at work so to obtain personal gain of any sort either for yourself or your friends, families or associates;

(f) use resources entrusted to you for the purpose not intended, and in an irresponsible and unlawful manner without obtaining authority;

(g) appropriate products or materials of the Group or its customers or suppliers for personal use by yourself, friends, family or associates;

(h) knowingly overcharge customers of the Group;

(i) fail to disclose information to another person where there is a legal duty to do so; and

(j) participate in any illegal activities, for example buying or selling stolen goods or allowing them to be kept on Group premises or premises of customers or suppliers of the Group.

6 RESPONSIBILITIES

6.1 You must ensure that you read, understand and comply with this policy.

6.2 The prevention, detection and reporting of fraud are the responsibility of all those working for us or under our control. All workers are responsible for:

(a) complying with this policy and the Group's Anti-Corruption and Bribery Policy (which is available on Sharepoint);

(b) acting with propriety in the use of the Group's resources and the handling and funds and those of customers and suppliers;

(c) being alert to the possibility that unusual events or transactions could be indicators of fraud;

(d) reporting details immediately if you suspect that a fraud has been committed or see any suspicious acts or events (see paragraphs 6.3 and 8 below regarding raising concerns); and

(e) co-operating fully during internal audits, reviews or investigations.

6.3 You must notify your manager as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future.

6.4 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for gross misconduct. We reserve our right to terminate our contractual relationship with all workers if they breach this policy.

7 RECORD-KEEPING

7.1 We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

7.2 You must declare and keep a written record of all hospitality or gifts, accepted or offered, which will be subject to managerial review and approval. Please refer to the Group's Anti-Corruption and Bribery Policy for further details regarding gifts and hospitality.

7.3 All accounts, invoices, memoranda and other documents and records relating to dealings with third parties, such as clients, suppliers and business contacts, should be prepared and maintained with strict accuracy and completeness. No accounts must be kept "off-book" to facilitate or conceal improper payments.

8 HOW TO RAISE A CONCERN

8.1 You are encouraged to raise concerns about any issue or suspicion of malpractice at the earliest possible stage. If you are unsure whether a particular act constitutes fraud or is otherwise unlawful, or if you have any other queries, these should be raised with your line manager or the Compliance Officer (which is the Group Legal Counsel). Concerns should be reported by following the procedure set out in our Whistleblowing Policy. A copy of our Whistleblowing Policy can be found at http://www.hsgplc.co.uk.

8.2 The Group's Fraud Risk Management Procedure in Schedule 1sets out the Group's policy and procedure regarding the deterrence, detection and investigation of fraud, including misconduct or suspected misconduct or dishonesty, by employees and others who interface with the Group. It also provides guidance regarding appropriate actions to take in the event of suspected fraud.

9 PROTECTION

9.1 Workers who refuse to participate in fraudulent activities, or those who raise concerns or report another's wrong-doing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

9.2 We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in fraudulent activity, or because of reporting in good faith their suspicion that an actual or potential fraud has taken place or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform the Compliance Officer immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our internal Grievance Procedure.

10 TRAINING AND COMMUNICATION

10.1 Training on fraud risk management forms part of the induction process to key employees, depending upon job title, current responsibilities and potential risks associated with that role, as required. Workers will receive regular, relevant training on how to implement and adhere to this policy.

10.2 Our zero-tolerance approach to fraud must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

11 WHO IS RESPONSIBLE FOR THE POLICY?

11.1 The board of directors has overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

11.2 The Compliance Officer has primary responsibility for monitoring the use and effectiveness of this policy and dealing with any queries on its interpretation. Management at all levels are responsible for ensuring those reporting to them are

made aware of and understand this policy and are given adequate and regular training on it.

12 MONITORING AND REVIEW

12.1 The Compliance Officer will monitor the effectiveness and review the implementation of this policy, regularly considering its suitability, adequacy and effectiveness. Any improvements identified will be made as soon as possible.

12.2 All workers are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrong-doing.

12.3 Workers are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Compliance Officer.

Roger McDowell

Chair

Gordon Banham

Group Chief Executive

Issue 1

January 2025

SCHEDULE 1 – FRAUD RISK MANAGEMENT PROCEDURE

AIM OF THIS PROCEDURE

The purpose of this Schedule 1 is to set out the Group's procedures regarding the deterrence, detection and investigation of fraud, including misconduct or suspected misconduct or dishonesty, by employees and others who interface with the Group. It also provides guidance regarding appropriate actions to take in the event of suspected acts arising.

RESPONSIBILITIES

Overall responsibility for the Fraud Risk Management sits with the Board. This includes the approval of this Fraud Risk Management procedure and ensuring that sufficient safeguards and frameworks are in place to allow for the effective detection and prevention of fraud. The Board is also required to approve the level of fraud risk appetite proposed by the Business Unit Managing Directors.

The Board may delegate the task of implementing this framework to the Business Unit Managing Directors, who will have effective day to day responsibility for:

- Proposing a suitable level of risk appetite in relation to fraud risk;
- Ensuring employees within their business unit are adequately briefed and trained with regard to fraud risk;
- Being aware of potential risks of fraud within their business unit;
- Enacting effective monitoring, review and control procedures to both prevent acts of fraud and detect acts of wrongdoing promptly should prevention efforts be unsuccessful;
- Ensuring learnings and feedback from suspected and confirmed fraud cases are appropriately rolled out within the business unit.

The authority to carry out the above responsibilities can be delegated to appropriate individuals within each Business Unit, however, the accountability for their effectiveness must remain with the Managing Director of the Business Unit.

Ultimately, it is the responsibility of every employee, consultant, agent and Director of the Group to immediately report any suspected fraud, misconduct or dishonesty, initially to their line manager or via the Group's whistleblowing hotline.

MONITORING OF FRAUD RISK

Fraud risk is a mandatory requirement for inclusion within all Business Unit Risk Registers. The identification and mitigation of potential fraud risks remains the responsibility of the Business Unit Managing Directors.

Risk Registers, including the identified Fraud Risks, will be reported to the Audit & Risk Committee regularly.

REPORTING INCIDENTS OF FRAUD OR WRONGDOING

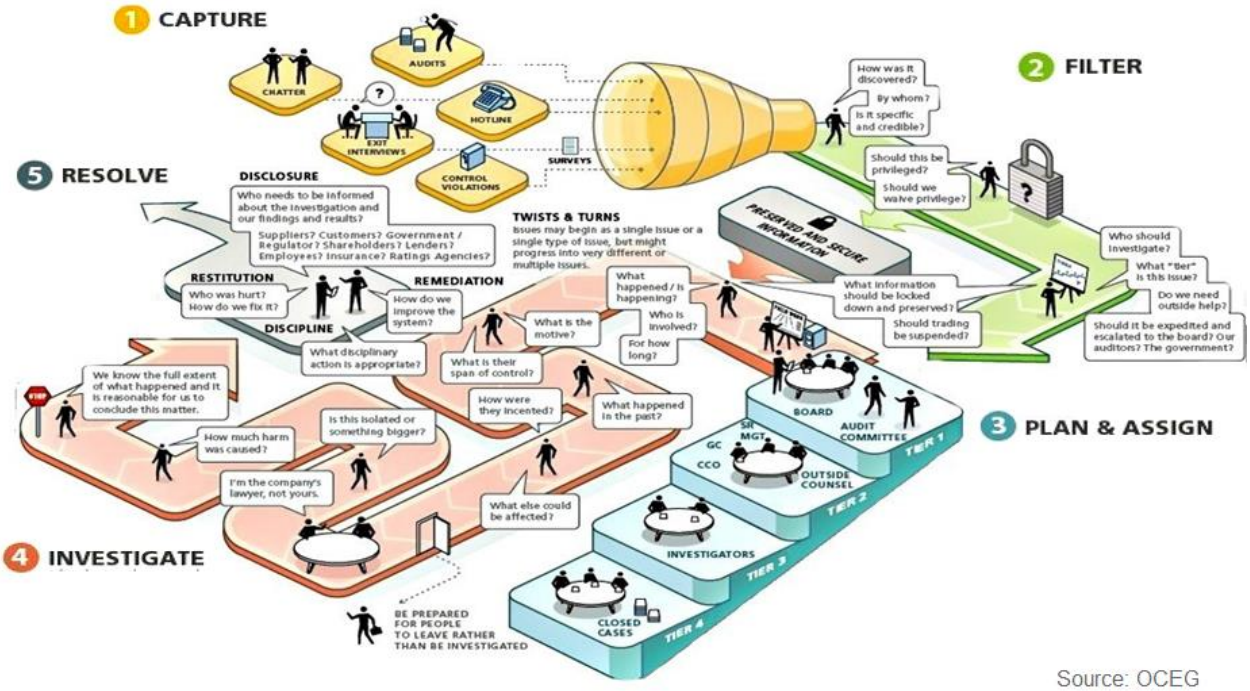
In cases of fraud, it is often information gathered within the first 48 hours which provide the most useful data to bring about a satisfactory conclusion, as this is often before the perpetrator has had time to react to the allegations.

It is the responsibility of every employee within the Group to immediately report any suspected fraud or misconduct to their line manager or via the Group's whistleblowing hotline. Managers upon being made aware of such potential acts must immediately report to the Compliance Officer (which is the Group Legal Counsel). Due to the important and yet sensitive nature of such suspected violations, it is essential we maintain a logical and professional approach to investigations. Employees, managers and directors must not perform their own investigation work outside of the process set out within this document, as that can be one of the biggest threats to correct and proper incident handling.

CONDUCTING INVESTIGATIONS

To ensure that all reported instances are treated equally and in a professional and independent manner the Group has agreed an investigation process which follows best practice guidelines from the OCEG (Open Compliance and Ethics Group).

The OCEG framework consists of 5 key areas to successful fraud investigation:



Source: OCEG

INVESTIGATION STAGES

Stage 1: Capturing information

Information relating to potentially fraudulent activities can be collected from a number of sources across the Group including:

- Reports to the whistleblowing hotline;
- Concerns raised to operational management;
- Information collected from exit interviews;
- Findings from internal and external audits;
- Control violations identified by management in day-to-day activities.

It is important that while we're capturing information relating to potential frauds that we make a conscious effort to avoid pitfalls such as:

- Not focusing on the full range of data sources, making sure that we don't miss a serious issue;
- Missing the 'big ones', making sure that we have the right (competent and independent) people in place to review and filter information as its received;
- Making everything a big issue;
- Assigning the wrong people to investigations, some investigations will require technical knowledge;
- Allowing management override of controls to interfere with the investigation or its objectivity;
- Carrying out a superficial investigation without getting to the root cause of the issue; and
- Destroying the chain of evidence.

At this stage all information reports received should be treated as confidential and forwarded to the Compliance Office, who will facilitate the initial triage process.

Stage 2: Filtering the information

Once a report has been received it is important that it is understood and filtered by a competent and independent source before the investigation begins. To help maintain a consistent approach the Compliance Officer (supported by additional independent individuals if required) will conduct a filtering exercise on all information received which will include:

- Ascertaining how the issue was discovered, and if it is specific and credible;
- Identifying who should be involved in the investigation (from an internal and external perspective); and
- Who needs to be made aware of the incident at this stage (e.g. the Board, external auditors, regulators etc).

After the initial investigation, the Compliance Office will make a decision in relation to further investigation of the reported issue.

Stage 3: Plan and Assign

Before any formal investigation can begin, an investigation plan (including planned communications), roles and responsibilities must be agreed. Roles and responsibilities should cover the investigation itself and the processing of any remedial issues identified during the investigation (even if the specific members of the operational team are not involved in the investigation itself).

Stage 4: Investigate

<u>Key considerations for the first 48 hours</u>

The first 48 hours of any investigation are critical, yet this is when many mistakes are made. During the first 48 hours it is crucial that we:

1. Fully understand the allegation
2. Identify the protocols, milestones and skills, and
3. Build the right team to fully investigate the issue.

Fully Understand the allegation

To enable a productive investigation, we need to first ensure that:

- The nature of the investigation is fully understood;
- Who may be involved in the incident, and what (if any) immediate operational changes need to be implemented;
- Which businesses of the Group may be affected;
- What data may be relevant, and how can it be secured;
- Potential commercial (or other) impact; and
- Who needs to be made aware of the allegation.

Identify the Protocols, Milestones and Skills

As part of the initial consideration of the investigation protocols, milestones, and skills needed to effectively investigate the incident must be established. For example:

Protocols	• **Privilege** • **Retention policies** • **Data privacy** • **Escalation**
Milestones	• Initial observations within 2 weeks • Agree frequency of further updates, and the most appropriate audience.
Skills	• Investigative interviewing skills • Forensic review and analysis • Financial modelling • Asset tracing • Business intelligence and background checks • Dispute readiness and advice • Forensic data technology • Experience in operational specialisms

	• Experience of subjects such as fraud, bribery and corruption, and counterfeiting.

Build the right team

The right investigation team will vary depending on the complexity of the incident being investigated. As with stages 2 and 3 the Compliance Officer will be responsible for coordinating stages 3 and 4.

Roles and Responsibilities

Specific roles and responsibilities will vary from investigation to investigation. However, they will reflect the roles and responsibilities detailed in the main body of this policy and will be formally agreed during the plan and assign stage of the investigation.

Stage 5: Resolve

As a result of each investigation a formal output will be produced, which at a minimum will detail the allegations, the findings of the investigation, and an outline of any identified issue which needs to be resolved by operational management.

CONFIDENTIALITY

The Group treats all information received with the utmost confidentiality. Any reprisal against any employee or other individual reporting an incident in good faith is strictly forbidden.

The identity of the employee who has brought the allegation will remain confidential. Investigation results will not be disclosed or discussed within anyone other than those who have a legitimate need to know within the bounds of the investigation. This is essential in order to avoid damaging the reputations of persons suspected, but ultimately found innocent and to protect the Group from potential civil liabilities.

DISCIPLINARY ACTION

If a fraud investigation results in the recommendation to dismiss or otherwise discipline an employee, the recommendation will be reviewed for approval by the appropriate representative from Human Resources and the Compliance Officer before such action is taken.

The Business Unit does not have authority to dismiss an employee for fraudulent activity without prior approval from the Compliance Officer.