



## **The Langstane Group**

### **Anti-fraud Policy**

Date approved by leadership team	25 June 2025
Board of management / committee name	Board of management
Approval date	21 August 2025
Review date	August 2028
Version	V4

<b>Version</b>	<b>Date approved</b>	<b>Changes</b>
Version 1	19 August 2019	New policy
Version 2	2 February 2021	An area of potential fraud will be reviewed quarterly and added to reports to the Audit & Governance Committee for consideration. Retain original date of review.
Version 3	August 2022	Change terminology to reflect organisational structure. Add examples and detail where required to augment and clarify requirements Add a section on Notifiable Events
Version 4	August 2025	Change to when police involvement and be initiated (previously only where there was evidence available, now ability to inform due to seriousness of potential fraud. 'Auditor' replaced with 'external professional' and 'significant' replaced with 'significant or otherwise' in Appendix 1

## 1. Introduction

Langstane Housing Association is a Co-operative and Community Benefit Society, and a registered social landlord with charitable status.

The Langstane Group (Langstane / the Group) consists of Langstane Housing Association Limited and its wholly owned subsidiaries.

This policy applies to all entities of the Langstane Group and to all those involved with the Langstane Group including all governing body members, employees, customers, consultants, contractors, agency employees, casual workers, volunteers and co-opted individuals.

For the purposes of this policy the term fraud includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. However, it essentially involves using deception to dishonestly make a personal gain and / or create a loss for another. It is important to note that fraud does not always involve money but can have other impacts, such as a loss of opportunity for housing applicants to access affordable housing.

There are service areas within housing associations that are of higher risk and these are detailed within this policy but that does not preclude other areas from being at risk of fraudulent activity.

It is important to recognise threats which present themselves from within the Langstane Group and those of an external nature. Some risks may fall across both areas.

The following are potentially higher risk areas for the Langstane Group:

Payroll	Cash handling
Procurement	Development
Finance function	Maintenance and repair
Recruitment	Cyber activity
Housing tenancy	

Section 5.2 of this policy details mitigation that is in place for these higher risk areas.

## 2. Aim of the policy

The aim of this policy is to ensure:

- Employees can identify which activities are higher risk and how they can be subjected to fraudulent activities;
- Employees know how they must act if they are, or they suspect they are, subject to such fraudulent activities;
- A corporate culture where employees feel engaged and have a stake in the success of the Group is developed and maintained. This reduces the likelihood of people deciding to commit fraud;
- Strong deterrents are in place for anyone committing fraud. This includes making routine fraud controls visible, and ensuring employees are aware of why those controls are in place;
- Fair but robust investigation processes and redress sanctions are in place; and
- The Langstane Group is protected from the effects of fraudulent activities.

### 3. Objectives

The Langstane Group is not defined as a regulated sector as it does not:

- Operate consumer credit activities under the Financial Conduct Authority (FCA);
- Provide any other form of lending including grant funding;
- Sell any property on behalf of another association; or
- Carry out any commercial activities on behalf of others.

Langstane Property Limited is required to register under the Money Laundering Regulations for supervision by His Majesty's Revenue and Customs (HMRC) to comply with letting agency regulations.

It is good practice to embed and maintain risk-sensitive policies and procedural controls that cover all activities that may be deemed higher risk. It is also vital to do so to protect the public investment in, and the reputation of, the social housing sector as a whole.

This policy will set out, in plain language:

- The risks faced by the Langstane Group and what are unacceptable actions;
- Any mitigation measures that can and must be undertaken;
- How to report any suspected fraudulent activities;
- What processes will be triggered if fraud is suspected; and
- How on-going monitoring and record keeping of higher risk activities will be undertaken and, when required, reporting of such activities to statutory / regulatory bodies.

### 4. Links to other strategic documents and policies

The Group's anti-fraud policy is linked to a number of strategic documents and policies in particular but not solely:

- Rules;
- Anti-bribery policy;
- Scheme of delegation;
- Financial regulations;
- Standing orders;
- Whistleblowing policy;
- Notifiable events policy;
- Entitlements, payments and benefits policy;
- Risk management policy;
- Safeguarding policy;
- Privacy policy and privacy notices;
- Information security policy;
- Code of conduct (for employees and governing body members);
- Declarations of interest - processes and registers;
- Employment handbook.

Any policy that relates to areas of higher risk of fraudulent activities will be explicit and mindful of the risks associated with the activity.

Where practical to do so, policies and procedures will reduce the likelihood of any inappropriate actions taking place by designing weaknesses out of processes and systems. For the avoidance of doubt, this includes the segregation of duties where practical and feasible to do so.

This does not remove the need for everyone connected to the Langstane Group to be vigilant to possible indicators that highlight fraudulent activities are taking place.

## 5. Policy

Anyone associated with the Langstane Group is expected to be above reproach in all aspects of their involvement. In keeping with the principles of good corporate governance and financial management, a zero-tolerance stance is taken against any activities that involve, or are likely to unduly expose, the Langstane Group to allegations of, or actual instances of, fraud.

Dependent on the nature of the activity, it may be appropriate to report fraudulent activity to the Scottish Housing Regulator and any other statutory and / or regulatory body.

Fraudulent activities constitute gross misconduct. Therefore Langstane Housing Association's disciplinary procedures will be instigated when any fraudulent activities are uncovered and any suspected fraudulent activities will be fully and thoroughly investigated.

Where direct evidence is available, **or the seriousness of any suspected fraud warrants it**, the police will be informed and full co-operation given during their investigations.

Where appropriate, the Group may instigate an independent investigation into the activity by a third party.

### 5.1 Fraud risk assessment

A fraud risk assessment is created that allows a high-level examination of higher risk Langstane Group activities detailing the management and control structures in existence.

This will assess the fraud risk profile and susceptibility to threats of fraud.

### 5.2 Mitigation

Mitigation is undertaken that is proportionate and risk based for roles that have a higher exposure to potential fraud. It is recognised that different roles, even those within the same team, may have higher exposure to fraud.

Adhering to and monitoring of internal controls is fundamental to overcoming fraudulent activity. The following sections detail what is in place for those higher risk areas identified in section 1 of this policy.

### 5.2.1 Payroll fraud

This can include:

- False claims for travel / subsistence by way of fictitious or inflated claims;
- False claims for work delivered, overtime, flexible working arrangements, allowances, one-off awards, special or ex-gratia payments or bonus payments;
- Non-existent or 'ghost' employees on the payroll that are used as a vehicle for payments to be made;
- Use of ex-employee or agency worker details which may be dormant on the system to make payments to a fraudster.

#### **Mitigation action that will be taken:**

- Accountability among management during budget setting and on-going monitoring so that ownership of budget headings is achieved. Training provided to ensure budget holders understand the detail of financial reports, how to interpret them and how they can be used to spot unusual variances that may be indicators of fraud;
- Ensuring the human resource function has an appropriate software system in place to accurately record, monitor and calculate time accrued; manage pay and leave entitlements; as well as providing a robust framework for audit and control of processes;
- Regular cleansing of payroll datasets to ensure accuracy and completeness;
- Receipts for subsistence required, and advance management approval for expenses above a specified threshold amount;
- Periodic use of data matching or data analytics to identify anomalies for further investigation;
- Segregation of duties / division of roles in approval processes;
- Robust approval procedures surrounding changes to employee personal details such as contact numbers, bank account details and changes in salary or allowances;
- Employee leaver notification processes in place to avoid salary overpayments.

### 5.2.2 Procurement fraud

Procurement activity sits in a framework and involves a complex set of processes. It is fundamentally important that any person involved in purchasing goods and services for the Langstane Group are fully trained, and has the knowledge and skills required and appropriate to their delegated authority limits.

Opportunities for procurement fraud are broad and need not involve any internal employees. It can be broken down to three phases.

### **Pre contract award phase:**

- Inadequate knowledge of, or biased research of the supply market limiting options towards certain products or suppliers;
- Circumventing thresholds to avoid formal structured procurement procedures. This is done via under-estimating contract values and then adding to it later, or splitting activity to limit total value;
- Shortcutting processes to limit time allowed for research and bidding – this is a particular risk in urgent or emergency situations;
- Specification tailoring / refinement by an insider or in collusion with a supplier to reduce the opportunities for suppliers to successfully bid for work – this is often a vehicle to award work to a single supplier;
- Operation of a 'cartel' or bid rigging, which involves a group of suppliers colluding to determined rates, or who will bid for specific pieces of work or contracts in a pre-defined sequence; Application of undue influence; offers of, or requests for, gifts and hospitality by suppliers to the procurement lead or decision maker;
- Risk of bribery by way of the procurement lead requesting or receiving an offer of a bribe which can be in the form of cash, goods, services or other inducements for their benefit or benefit to another;
- Conflicts of interest (actual, perceived, or potential) not being declared.

### **Mitigation action that will be taken:**

- Segregation of duties involving the development of tender specifications where practical;
- Use of independent specialist advisors where the skillset for the development of tender documentation requires it instead of seeking template specifications from suppliers who may potentially bid for the work;
- Mandatory and positive returns for the declaration of interests for any parties / panel members involved in the review stages, assessment or interview panels;
- Mandatory expectation of suppliers to declare commitment to the Langstane Group's anti-bribery policy;
- Clear senior position statement surrounding the Group's stance on approaches for inducements or attempts to influence the process by suppliers;
- Robust processes are in place for reviewing total contract values when costs are adjusted after contracts have started. This includes documenting all justifications for any changes made;
- Ensuring invitations to bid are sufficiently wide to ensure genuine competition;
- Conduct regular audits of procurement activity.

**Tender or negotiation phase:**

- Risks of inducements or bribes;
- Undue influence over processes by prospective suppliers / bidders;
- Avoidance of set processes for gain or advantage.

**Mitigation action that will be taken:**

- Sample audit of tender procedures against specific projects;
- Audited reviews into procurements / purchases;
- Due diligence and conflict of interest verification by independent parties / auditors;
- Clear and controlled bid processes which are transparent and auditable;
- Robust measures for on-going declaration of interests;
- Segregation of duties / multi-layered approach to decision making, with clearly documented scoring matrix / logs or rationale for appointments;
- For contracts above a set threshold value or of a specialist nature, appointment of an independent person or procurement lead to facilitate arrangements around procurement processes who is not involved in the decision making;
- Setting clear expectations and stance of the Langstane Group surrounding gifts and hospitality;
- Not assuming a complaint from an unsuccessful bidder is 'sour grapes' and following the Group's complaints procedure in all cases where dissatisfaction with the procurement process is expressed;
- Transparent and witnessed / documented negotiation procedures.

**Post contract delivery, monitoring and management:**

- Non delivery against specification or the Langstane Group's expectations;
- Unclear, or unsubstantiated additional costs invoiced or claimed outside of the contract;
- Mischarging for costs and / or labour;
- Manipulation of contractual terms previously agreed;
- Inflation of costs / overruns on budgets.

**Mitigation action that will be taken:**

- On-going due diligence of higher risk suppliers to ensure the Langstane Group's reputation and finances are protected;
- Supplier contracts have clear audit clauses. These are proven to be effective mechanisms in fraud prevention;
- Clear contract management in place assigned to a named person for accountability;
- Joined-up approach for verification of invoices prior to payment to ensure goods and services have been delivered, and to expected standards;
- In instances of long-standing tenders, clear handovers between employees that enables the contract to continue against contractual obligations;

- Sample testing / audit of processes and documentation by specialist employees / auditors;
- Contract terms clearly state that change of ownership must be declared in advance of such transfer of ownership taking place.

### 5.2.3 Finance function fraud

The finance function is a key function of the Langstane Group. There are several higher risk areas that may be targeted for fraudulent activities including:

- Invoicing;
- Accounts manipulation and misreporting;
- Account takeover by fraudsters (internal and external);
- Use of dormant supplier lists to facilitate fraudulent payments;
- Supplier set up / changes to supplier details;
- Mandate / bank account fraud;

#### **Mitigation action that will be taken:**

- Updated and regular fraud awareness and scam awareness sessions for employees within this function;
- Enhanced pre-employment screening of people who apply, or are engaged as temporary cover, for certain posts ;
- Regular cleansing of dormant / infrequent suppliers from system, and checks for any new suppliers being added to the system;
- Conflict of interest checks at the outset of engagement and on-going obligation for updates or changes to be made;
- Use of purchase orders to facilitate payments to suppliers;
- Robust measures surrounding access to supplier details and changes made, such as bank account changes or contact details. These have a defined authorisation and pre-payment verification processes;
- All policies are strictly followed e.g. financial regulations, standing orders;
- Authorised signatories / authority levels are enforced;
- Signatories list is maintained and updated;
- Duty separation wherever practical and implementation of internal checks;
- Ability to swap employees, or enforcement of holiday breaks, to enable another post holder to undertake a person's role as an effective measure to identify potential fraudulent behaviours / system weaknesses;
- Implementation of recommendations of internal audit / best practice;
- Monitoring of budgetary control;
- IT controls / security of financial systems;
- Controlled access to offices and records;
- Use of approved suppliers / original invoices;
- Sample review of payments either side of financial approvals threshold;
- Data analytics / data matching against payroll and third-party datasets where possible;

- Clearly defined incident response plan, accessible to all employees within the service.

#### 5.2.4 Recruitment fraud

Recruitment fraud can include:

- False identities / identity theft;
- False or exaggerated qualifications or experience on application for employment;
- Undisclosed convictions or regulatory sanctions;
- False references;
- Use of forged, manipulated or stolen documents;
- Illegal workers / entitlement to work issues.

#### **Mitigation action that will be taken:**

- Robust recruitment processes and procedures underlined by a clear policy and best practice. This includes the employment of new starters, TUPE transfers, secondments and volunteers;
- Employees trained in the identification of fraudulent documents, red flags on application forms;
- Proportionate background checks and due diligence undertaken for applicants. On-going / periodic due diligence carried out for higher risk roles and for senior employees;
- Fraud response plan invoked when appropriate e.g. when recruitment fraud is suspected;
- Employees kept apprised of trends in recruitment fraud.

#### 5.2.5 Cash or payment voucher handling fraud

This can include:

- Theft of cash by employees from within the petty cash float / system;
- Abuse of system to obtain payment vouchers for personal gain, or distribute vouchers in a fraudulent manner;
- Cash collection area thefts;
- Theft following doorstep collection of rental or other income due to the Langstane Group;
- Abuse of funds / theft of cash from tenants, often vulnerable tenants, whereby employees have access to tenant premises or ability to access funds held by tenants.

#### **Mitigation action that will be taken:**

- Robust action taken when management controls are overridden;
- Cash handling / voucher processing procedures routinely audited with occasional unplanned / un-notified reviews;
- Cash handling procedures promoted to ensure cash is received and deposited in a secure, timely and effective manner;
- Cash handling training provided to employees, incorporating associated policies and procedures;

- Cash is secured in a safe before banking and cash is not kept in uncontrolled / insecure areas;
- Tenant rent account information routinely audited;
- Individual employees do not have control over two or more steps in the cash and payment voucher handling / banking procedures.

#### 5.2.6 Development fraud

This can include:

- Collusion between employees and contractors;
- Increased or high value gifts, hospitality and inducements offered or requested;
- Relationships between contractors and employees engaged in the procurement or contracting process where conflicts of interest exist but are not declared;
- Increased costs above budget incurred where the explanation or reasoning is unclear;
- One-off or special exceptional costs not planned or expected are requested;
- Land valuations are not in line with other transactions / local land charges;
- Projects or services are not delivered in full, or not delivered to specification;
- Bribes or 'kickbacks' offered by suppliers;
- Money laundering risks associated with high value transactions.

#### **Mitigation action that will be taken:**

- Use of frameworks of professional advisors who have been subject to due diligence checks;
- Clear segregation of duties with supply chain relationships;
- Data analytics of payments against datasets held within organisation if available;
- More than one employee attends contract management meetings to ensure risks are minimised (for example a note taker);
- Prior and on-going due diligence of suppliers;
- Robust contract management and periodic audit arrangements in place;
- Robust gifts and hospitality policies and registers in place with frequent reviews conducted;
- Clear declarations of interest policies and registers maintained which are subject to periodic review and oversight;
- Clear anti-bribery statements built into contractual terms which suppliers are required to commit to.

#### 5.2.7 Estates and maintenance fraud

The types of fraud that can occur include:

- Collusion between employees and contractors;

- Inferior materials or counterfeit product being used in replacement of legitimate parts or supplies;
- Over or undersupply of materials or services;
- Theft of materials or equipment;
- Undertaking authorised private work during working day;
- False / double invoicing;
- Invoicing for work or provision of services outside of contractual terms and conditions;
- Relationships between contractors and employees engaged in the procurement or contract process where conflicts are not declared;
- Increased costs above budget incurred, where the explanation or reasoning is unclear;
- One-off or special exceptional costs not planned or expected, are requested;
- Land valuations are not in line with other transactions / local land charges;
- Projects or services not delivered in full, or not delivered to specification;
- Bribes or 'kickbacks' offered by suppliers;
- Money laundering risks associated with large value transactions;
- Circumnavigating procurement limits on contract value to allow an employee to manipulate system and elect a contractor of choice.

**Mitigation action that will be taken:**

- Business cases to support expenditure of high-value items or projects required;
- Robust contracts with clear, easy to understand details of what services / goods are included / not included;
- Right to audit clauses and anti-bribery statements contained within contractual terms and conditions;
- Management information and budget reports reviewed regularly, outlining expenditure against expected forecasts;
- Random verification of works delivered;
- Random invoice testing for details of costs compared against contracted terms;
- Data analytics of payments against datasets held within the Langstane Group and third-party datasets, if available.

**5.2.8 Tenancy fraud**

Tenancy fraud takes many forms including:

- Fraudulently obtaining a social tenancy;
- Joint tenancy fraud;
- Unlawful non-occupation (abandonment);
- Unlawful occupation (subletting or key selling);
- Wrongly claimed succession.

### **Mitigation action that will be taken:**

- Publicising and applying consistently a zero tolerance policy for unlawfully obtaining / subletting / succeeding a tenancy, and using newsletters and the website / social media to assist tenants and others to identify and report fraudulent activity they may witness;
- Robust checking methods and photographic identification used to ensure applicants are who they claim to be, they are in need of the property, and they are entitled to social housing;
- Background and tenancy checks undertaken where possible to ensure other properties are not leased or owned by the applicant(s) that can be used as their principle home;
- Clear segregation of duties between those applying for housing / housing services, and those that process such applications / services;
- Employees are trained to identify false applications / requests for services / red flags for all types of tenancy fraud;
- System checks to identify third party payments on rent accounts, accounts that are excessively in credit, no contact for repair and maintenance, and unknown persons signing off repairs;
- Targeted visits to older and / or more vulnerable tenants to accurately capture and record who resides at the property (no more than 12 months apart);
- Allocation policy clearly defines action that may be taken if fraudulent activity is discovered;
- Where necessary and appropriate, checks will be made to confirm occupancy.

### 5.2.9 Cyber fraud

Cybercrime or fraud is any criminal act dealing with computers and networks (sometimes referred to as hacking), or where a computer is used to facilitate fraud. This also includes more traditional crimes conducted through the internet.

Cyber fraud may be possible due to:

- Increasing network connections and dependencies;
- Increasing sophistication of attackers (use of viruses, worms, ransomware, phishing, password loggers);
- Rise of social media;
- Increase in data held electronically including bank account details, next of kin, addresses;
- Under reporting / detection of incidents;
- Overuse of same password for multiple platforms;
- Value of data traded by organised groups;
- Demands being made to prevent a threatened cyber-attack (cyber extortion).

### Mitigation action that will be taken:

- Information Security Policy in place, and periodic audits to ensure policy is being adhered to;
- Risks of cyber fraud identified, and on the appropriate risk register;
- All software and operating systems kept fully updated;
- Regular employee training undertaken to recognise and deal with potential attacks;
- Data scrubbing exercises carried out as appropriate;
- Good basic IT controls are in place that prevent exposure to cyber-attacks;
- Policies and procedures periodically reviewed with a view to cyber fraud prevention, detection and reaction;
- Employees deliberately circumventing systems that may impact on the Group's IT security are robustly dealt with under Langstane Housing Association's disciplinary policy;
- Firewalls, operating systems and virus engines are kept up to date;
- An effective patch management programme in place;
- Software no longer utilised is removed completely from the Langstane Group's systems;
- All software and Wi-Fi password protected with multi-factor identification where appropriate;
- IT disaster recovery plan in place for when an incident occurs;
- Cyber essentials will be complied with;
- Cyber insurance in place;
- Physical site controls checked randomly and such checks recorded;
- All accounts and access rights are deleted when a connection to the Langstane Group ends;
- Penetration tests undertaken.

### 5.3 Key fraud indicators

As with most crimes, there are often behaviours present that, had they been recognised as 'red flags', may have either prevented the incident or at least uncovered it sooner. However, it is important to note that not everyone exhibiting 'red flag' indicators will be involved in fraudulent activities.

Examples of key employee fraud indicators, or 'red flags' are:

Behaviour	Results / KPIs	Documentation	Indicators
Sudden change in lifestyle	Always meets budgets	Lost documentation	Bullying individuals
Extravagant spending	Always reports early	Erased or crossed out figures	Unusual business structures / reporting lines
Does not take holidays / refusal of promotion	Erratic performance	Unusual fonts and inconsistent type faces	Regular visits by same suppliers / excessive hospitality

Behaviour	Results / KPIs	Documentation	Indicators
Unusually stressed Backlogs of work Lives beyond means Increases number of hours worked First in, last out Controlling (particularly 'experts')	Unexpectedly consistent results High volumes of cash transactions Write-offs outside normal limits or high volumes	High number of transactions of the same amount High levels of credit notes Poor tendering and selection processes Photocopies when originals would be expected Clearly falsified documents Documents rewritten (on pretext of neatness) Lack of detail on documents	Unusual employee turnover (high or low) Concerted efforts to avoid audit Employee asks for a loan / has a wage arrestment in place Unusual terms and conditions agreed Expense claims outside normal levels

#### 5.4 Unacceptable actions

The following are deemed unacceptable for anyone connected to the Langstane Group in a professional capacity, including any volunteer work undertaken:

- Accepting or asking for a bribe, whether financial or otherwise, from any person or organisation in return for providing a favour(s) whether or not the required favour(s) is within the remit of the individual to deliver;
- Offering a bribe, whether financial or otherwise, to any person or organisation in return for providing a favour(s) whether or not the required favour(s) is within the remit of the individual or organisation to deliver;
- Making or accepting any payments, or the instruction of any payments to be made or received, which are out with the terms of a contract (either employment or work related) or in terms of agreed policies (such as the entitlement, payments and benefits policy) for gain;
- Carrying out / speeding up / slowing down any routine procedure(s) for gain;
- Dishonesty, theft, fraud, or the deliberate falsification of records and / or benefit / or other claims;
- Falsifying records for any purpose including time sheet / attendance records;
- Using work time to carry out non-work activities;
- Taking goods for personal or commercial use including doing 'homers';
- Using work resources or materials for non-work activities including furthering alternative employment;
- Using Langstane Group systems to gain access to information out with remit and / or to gain unfair advantage e.g. in allocation of properties for rent or sale;

- Accepting full or part payment of large transactions in cash (£2,500 and over), where the provenance of such funds is not provided or the legitimacy of such funds is doubted;
- Allowing the introduction of unknown parties to any transaction at a late stage;
- Allowing the submission of suspiciously low tenders in competitive tendering exercises;
- Accepting suspiciously high tenders in competitive tendering exercises where other bidders have withdrawn.

The above list is not exhaustive.

Care will be taken when accepting hospitality and especially whilst procurement activities are being undertaken when the acceptance of hospitality should be avoided.

The entitlements, payments and benefits policy will be followed at all times.

Any actual or attempted fraudulent activity on the part of anyone associated with the Langstane Group or undertaken due to their negligence or inappropriate actions, amounts to gross misconduct. Where there is direct evidence of fraud the police will be involved and full co-operation given by the Group to ensure a thorough investigation takes place and if appropriate, prosecution secured.

The Langstane Group reserves the right to carry out an independent internal or external investigation.

Care will be taken to ensure any allegations of possible fraud are not made maliciously and are based on reasonable assumptions of fraudulent activity taking place and the matter raised in good faith. Where malicious allegations have taken place, these may be dealt with under the Group's disciplinary policy and if appropriate, action taken against the person(s) making the allegations.

## 6. Notifiable events

The Langstane Group has a notifiable events policy that will be read in conjunction with this policy.

As a general guideline, notifiable events are those that may:

- seriously affect the interests and safety of tenants, people who are homeless or other service users;
- threaten the stability, efficient running or viability of service delivery arrangements;
- put at risk the good governance and financial health of the Association;
- bring the Association into disrepute or raise public or stakeholder concern about the Association or the social housing sector.

Taking the above into account, it is possible that a breach of this policy is reportable as a notifiable event. This could be due to reputational damage should the breach become public knowledge, or in relation to dismissal of an employee, or legal proceedings.

The leadership team will consider breaches on a case-by-case basis and make a decision taking into account the current Scottish Housing Regulator guidance on notifiable events. In most cases the notification is made by the chief executive or, in some circumstances, the chair of the board of management, or their deputy, will submit the notification to the Scottish Housing Regulator.

## 7. Roles and responsibilities

### 7.1 Board of management and chief executive

Overall responsibility for fraud prevention lies with the board of management with day-to-day implementation and adherence delegated to the chief executive.

The board of management is responsible for ensuring:

- Effective risk management controls and procedures are in place that deter, detect and report suspected fraudulent activity;
- A workplace culture that promotes stakeholder buy-in, increases employee motivation, and reduces the likelihood of fraud is operated at all times; and
- All reported incidents of suspected fraud are promptly and robustly investigated and where necessary, appropriate sanctions and redress applied.

The board of management is responsible for ensuring its actions meet the highest standards and in particular the Scottish Housing Regulator's regulatory standards for governance and financial management and the approved code of conduct for governing body members.

The role of the joint audit and governance committee is detailed within its remit and includes:

- Monitor the integrity of the financial statements; and
- Review internal financial controls and risk management systems.

The above includes the review of internal and external audit reports.

The joint audit and governance committee will receive an analysis of an area of fraud on a quarterly basis. This will detail the measures taken to alleviate the risk of fraud against the Langstane Group.

Where fraudulent activity is strongly suspected or an allegation received, the chief executive will be advised immediately and will set up a fraud response team. This will normally include the director of finance and corporate services and another member of the leadership team. Where the allegation relates to the chief executive, the chairperson of Langstane Housing Association will be advised and will instruct the actions to be taken.

The convenor of the joint audit and governance committee will be advised immediately as will the chairperson of Langstane Housing Association and the chairperson of any directly affected subsidiary.

The chief executive will implement the fraud response plan (see Appendix 1) and notify any required regulatory body including but not restricted to the Scottish Housing Regulator.

## **7.2 Leadership team (chief executive and departmental directors)**

The leadership team has responsibility for ensuring robust working practices are in place that mitigate against the possibility of fraud and for signing annual anti-fraud statements. These confirm to the best of their knowledge and belief, effective policies, procedures, and controls systems, are in place for deterring, detecting, and reporting, fraud; and these are working effectively and are periodically reviewed in accordance with good practice.

The leadership team are responsible for ensuring:

- Governing body members receive up-to-date, accurate information in relation to good governance and financial management and expected standards of conduct;
- A culture of transparency and honesty is fostered amongst employees, and ensuring they are aware of the expected standards of professional conduct required;
- Employees have the required level of knowledge and training to undertake their roles and are trained in the respective policies, procedures and systems that contribute to the Group's anti-fraud policy;
- All anti-fraud measures are adopted across the board; and
- The notification requirements of regulators are met.

Individual members of the leadership team have roles in relation to the fraud response plan and the Group's whistleblowing policy.

## **7.3 Employees**

Individuals must adhere to the approved code of conduct for employees at all times. They are also tasked with:

- Being alert to possible triggers and higher risk areas of business that may be targeted for fraud within their area of work;
- Reporting any suspicious activity or suspected / attempted fraudulent activity;
- Acting with integrity and propriety at all times.

In addition, employees must report immediately to their line managers, any areas of weakness in systems and / or processes and, if known, any suggested ways of reducing / eliminating the possibility of fraud.

## 7.4 Auditors

The above does not replace the role of the Langstane Group's auditors, both internal and external. Nor does the use of internal and external auditors remove responsibility from those connected to the Langstane Group.

Internal auditors are employed to support the detection of fraud through testing the appropriateness, adequacy and effectiveness of relevant policies and procedures. The Group's external auditors, who by examination of the financial statements annually, identify any audit and accounting issues and assess the effectiveness of internal controls.

## 8. Reporting, monitoring and review

The Group's whistleblowing policy details the ways in which employees, governing body members, and others associated with the Langstane Group, may raise concerns about activity they feel is inappropriate. Notwithstanding that policy, the chief executive must be informed as soon as practical of any suspected fraudulent activity unless such suspicions relate to the chief executive in which case concerns may be raised with Langstane Housing Association's chairperson.

## 9. Equality and diversity

The Langstane Group is committed to promoting equality and diversity across all areas of work. Discrimination or harassment of any kind is not tolerated.

If you would like this document in large print, please contact Langstane's customer service team on 01224 423000.

### Fraud response plan

The purpose of the fraud response plan is to set down a consistent process to be followed in the event of a suspected fraudulent activity within the Langstane Group. This will ensure matters are dealt with in a timely manner and show how employees will investigate, report and close incidents when they occur, avoiding errors and providing structure.

### Initial report of suspected fraud

Where a report of suspected fraud is made, the chief executive will be advised without delay. In the chief executive's absence the director of finance and corporate services will be advised and they will advise the convenor of the joint audit and governance committee.

The chief executive will, as soon as possible and normally within 24 hours, convene a meeting of the fraud response team and start a log of actions. The fraud response team will normally have as its membership, the chief executive, the director of finance and corporate services and the director responsible for the area of suspected fraudulent activity.

The fraud response team will decide on the initial action to be taken. This may include:

- Deciding whether or not an investigation is necessary, and if it is, engage an investigating officer (this may be an employee or an **external professional**. If an employee, the person chosen will be appropriately experienced and independent of the activity affected by the suspected fraud);
- Any additional resource required to support the investigation (this may be revisited during the investigation);
- Any immediate requirement to notify the police and / or seek legal advice and if there is, who will lead on this and what will be disclosed (this will be revisited during the investigation);
- The need to inform the external auditor of the matter, and agree arrangements for keeping them advised of progress;
- The need to inform the Group's insurers, who will be lead on this, and what will be disclosed;
- Consider how to secure records / assets to prevent further loss and to preserve evidence;
- Consider membership of the fraud response team and whether or not the team needs to be expanded;
- Agree whether or not any regulatory notifications are required and those responsible for making such notifications;
- Agree whether or not any other notifications are required, e.g. lenders, and those responsible for making such notifications;
- Document the agreed steps to be taken, preparing a brief for the investigator which details the objectives of the investigation; and
- Agree how often the joint audit and governance committee convenor will be kept up to date by the chief executive.

Likely objectives of any investigation may include:

- Identifying the culprit(s);
- Establish the facts surrounding the fraud;
- Ascertain the total losses (where appropriate);
- Remove the threat of further losses;
- Obtain sufficient evidence for successful disciplinary, criminal or civil action;
- Return or retention of the property.

## Initial investigation

Discretion will be used at all times.

The Investigator will create an investigation plan setting out what information is required and from whom; and conduct an initial information gathering exercise to enable the circumstances to be thoroughly investigated and completed without delay.

Findings will be reported to the fraud response team alongside any interim conclusions. If required, an action plan will be provided to guide the next steps to be taken.

The information provided will, at all times be kept confidential within the fraud response team, and only shared where absolutely necessary with those who have a legitimate need to be involved.

In circumstances where an allegation of fraud has been made, and subsequent investigations do not substantiate such an allegation, every effort will be made to minimise any potential damage to the individual's reputation.

Where initial investigations establish reasonable grounds to suspect internal fraud has occurred and the level of potential fraud warrants it, or where external fraud is suspected, the Group's policy is to advise the police at an early stage.

Where the police wish to advance investigations, full co-operation will be given and clear lines of communication will be agreed with the chief executive.

Where the police do not wish to take forward further investigations, the fraud response team will agree a way forward internally.

An objective of any fraud investigation will be to ensure an appropriate sanction against any perpetrator and to recover, where practical, any losses to the Group.

Where an employee is involved, either directly or through negligence, **significant or otherwise**, which contributed to any fraudulent activity, the Group will instigate disciplinary processes and if practical, pursue the prosecution of anyone involved.

## Further investigations

Where initial investigation provides reasonable grounds for suspecting an employee of fraud, the fraud response team will reach a decision on whether or not the individual(s) involved should be suspended. Any decision will be taken and action carried out to suspend an

employee to protect both the employer and employee and to prevent the suspect(s) from destroying / removing evidence or undertaking further fraudulent activity.

In the circumstances, those involved will be approached without warning and supervised, at all times, to leave the building. Their access to any documents, electronic or otherwise, will be removed immediately. Nothing other than personal belongings may be removed and their keys, mobile devices, and any other property of the Group will be returned prior to leaving the building.

If no suspension is undertaken at the beginning of the investigation, the fraud response team will review this decision periodically during the continued investigation.

It may be necessary to widen the scope of the investigation if it is subsequently thought the issue to be more widespread. This will again, be reviewed periodically throughout the investigation.

Where technical expertise is required, the fraud response team has responsibility to appoint external specialist to lead or contribute to the investigation. Due to the nature of the investigations, there is justification for this not being subject to external tender.

At all times, employees interviewed who are under suspicion will be advised if the interview is formal or informal and they will have the right to be accompanied. It will be explained that no pre-set view has been made but the allegation will be outlined and the employee given sufficient time to respond. All meetings will be carefully and accurately recorded.

If formal questioning is needed because involvement in a criminal offence is suspected, then the interview will be conducted in accordance with the principles of the relevant legislation in place at the time.

### **Applying sanctions**

A range of sanctions will be considered ranging from:

- Internal disciplinary action;
- Regulatory involvement if they are a regulated profession e.g. accountant;
- Prosecution; **and** / or
- Private prosecution using a specialist law firm.

All sanctions will be accurately documented and applied consistently.

### **Recovery of losses**

Where possible the Group will aim to recover losses in all circumstances. Where the loss is substantial, legal advice will be taken and if possible, the assets of the individual(s) frozen through court action, pending the conclusion of investigation(s).

Where recovery is against a customer or other third party, legal proceedings will be instigated. If the Group takes legal action, recovery of expenses will be advanced.

The fraud response team will decide on whether or not a claim under the Group's insurance policies is appropriate but this will be a last resort.

## **Case closure and reporting findings**

On completion of any investigation(s), a written report will be submitted by the investigator to the fraud response team. This will contain:

- A summary of the brief;
- Details regarding the incident, those involved, and how the fraud was able to be undertaken and how it was detected;
- Measures required to prevent a recurrence;
- Quantify the losses incurred;
- Progress on recovery action, disciplinary action and, if appropriate, criminal action;
- Actions that would detect similar incidents.

The report will be submitted to the next joint audit and governance committee or in the event of a significant issue occurring, a special meeting of the joint audit and governance committee will be convened to hear the report. This will then be reported to the next board of management meeting alongside details of when any required changes to policies and procedures are to be made to prevent further incidents taking place.

Where the regulatory notification is required, this will be undertaken as soon as practical.

## **Communication**

All communication regarding the investigation will be dealt with by the chief executive. No other person involved with the investigation or with the Group has authority to discuss the matter internally or externally.

## **Review**

The fraud response plan will be reviewed every three years or following an incident to ensure it is fit for purpose and provides clarity on process, etc.